POINSOT

SUR LA THEORIE DES NOMBRES

N. 16



RÉFLEXIONS

SUR LES

PRINCIPES FONDAMENTAUX

DE

LA THÉORIE DES NOMBRES.

OUVRAGES DE M. POINSOT.

ÉLÉMENTS DE STATIQUE, suivis de quatre Mémoires sur la Composition des Moments et des Aires, sur le Plan invariable du Système du Monde, sur la Théorie générale de l'Équilibre et du Mouvement des Systèmes, et sur une Théorie nouvelle de la Rotation des Corps; 8e édition, considérablement augmentée, vol. in-8°, avec planches, 1842. *Ouvrage adopté pour l'Instruction publique.*

RECHERCHES SUR L'ANALYSE DES SECTIONS ANGULAIRES; vol. in-4°, 1825.

MÉMOIRE SUR LES POLYGONES, etc.; in-4°.

SUR LA COMPOSITION DES MOMENTS ET SUR LA THÉORIE DE L'ÉQUILIBRE ET DU MOUVEMENT DES SYSTÈMES; in-4°.

MÉMOIRE SUR L'APPLICATION DE L'ALGÈBRE A LA THÉORIE DES NOMBRES; in-4°.

IMPRIMERIE DE BACHELIER,
rue du Jardinet, 12.

RÉFLEXIONS

SUR LES

PRINCIPES FONDAMENTAUX

DE

LA THÉORIE DES NOMBRES,

PAR M. POINSOT,

Membre de l'Institut et du Bureau des Longitudes, Membre du Conseil royal de l'Instruction publique, Commandeur de l'Ordre royal de la Légion d'honneur, etc.



PARIS,

BACHELIER, IMPRIMEUR-LIBRAIRE

DE L'ÉCOLE POLYTECHNIQUE, DU BUREAU DES LONGITUDES, ETC.,

Quai des Augustins, nº 55.

—

1845.



RÉFLEXIONS

SUR

LES PRINCIPES FONDAMENTAUX

DE LA THÉORIE DES NOMBRES,

PAR M. POINSOT.

(Extrait du *Journal de Mathématiques pures et appliquées*, tome X, 1845.)

I.

Je me propose de parcourir et de démontrer dans cet écrit les principales propositions qui servent de base à la théorie des nombres. Quoique les géomètres en aient déjà donné des démonstrations plus ou moins ingénieuses, je ne crois pas inutile d'en présenter encore de nouvelles, qui me paraissent à la fois plus simples et plus directes, ou qui, étant tirées d'un nouvel ordre de considérations, sont propres à mettre la doctrine dans un nouveau jour [*].

[*] J'avais jeté sur le papier ces réflexions et ces démonstrations relatives à la théorie des nombres, dans la seule intention d'éclaircir, pour quelques personnes, les premiers principes de cette importante théorie. On m'a persuadé qu'il pouvait être utile de les publier; mais je prie le lecteur de les recevoir avec indulgence, parce que je les donne ici telles qu'elles se sont présentées dans le cours de cette espèce de conversation mathématique.

Ces démonstrations pourraient entrer facilement dans nos ouvrages élémentaires, et par là contribuer, bien plus qu'on ne l'imagine, aux véritables progrès de la science. Car si la théorie des nombres est encore peu avancée, malgré les efforts des plus grands géomètres, ce n'est point uniquement à la difficulté propre de la matière qu'on doit attribuer la lenteur de ces progrès : elle tient peut-être encore plus à cette espèce d'isolement et d'abandon où l'on a laissé jusqu'ici cette première partie de nos études mathématiques. Il faut observer que la théorie des nombres est tout à fait négligée dans nos Éléments, et que l'esprit ne s'y exerçant pas d'assez bonne heure, n'est peut-être plus capable de s'en rendre ensuite les principes assez familiers. Les Anciens y donnaient plus de soin dans leurs ouvrages; on dirait qu'ils en avaient mieux senti l'importance, et leurs livres, à cet égard, ont encore de l'avantage sur les nôtres. Mais depuis longtemps il semble que les auteurs aient regardé la théorie des nombres comme une spéculation singulière, qui ne se lie à rien ni dans l'Analyse ni dans la Géométrie, et qui n'offre ainsi à l'esprit que des vérités plus curieuses qu'utiles. A peine en trouve-t-on quelques traces dans les Traités ordinaires d'Arithmétique et d'Algèbre. Et cependant, pour peu qu'on y veuille réfléchir, il est aisé de voir que cette arithmétique transcendante est comme le principe et la source de l'algèbre proprement dite. C'est une vérité qu'on pourrait établir par le raisonnement, comme je le montrerai tout à l'heure, mais qu'on peut aussi prouver en quelque sorte par l'expérience. Car, observez que ce peu qu'on ajoute de temps à autre à l'algèbre vient du peu qu'on découvre par intervalles dans la science des propriétés des nombres. On en a surtout un bel exemple dans cet heureux rapprochement qui a fait connaître à M. Gauss la résolution algébrique des équations binômes de tous les degrés, et la nature des nombres premiers par lesquels on peut diviser régulièrement le cercle au moyen de la règle et du compas. C'est un pas inattendu et bien remarquable, que la théorie des nombres a fait faire à la fois à l'algèbre et à la géométrie. L'algèbre, à son tour, par ses signes, et la géométrie même, par ses figures, peuvent s'appliquer aussi heureusement à la théorie des nombres, y faire éclore de nouvelles idées et de nouveaux théorèmes, indiquer de nouvelles routes dans la science, et nous apprendre enfin quelque chose sur l'art encore inconnu de nous y con-

duire. C'est ce que j'ai tâché de montrer d'une manière assez frappante, dans un Mémoire étendu où j'ai donné le premier essai de cette singulière application, et où l'on a vu les imaginaires mêmes servir à la représentation analytique de certains nombres dont la loi nous était entièrement inconnue [*].

Ces rapprochements et quelques autres semblables montrent assez la liaison de l'algèbre et de la théorie des nombres; mais, comme je l'ai dit plus haut, c'est ce qu'on peut voir aussi, indépendamment de ces exemples, et pour ainsi dire à priori, en s'élevant à l'idée qu'on doit se faire de la science mathématique considérée de la manière la plus générale. Cette réflexion mérite d'être développée.

II.

On définit ordinairement les mathématiques la science des *grandeurs* en général, ou la science des *quantités*, c'est-à-dire, au fond, la science des *rapports*; c'est la définition la plus générale qu'on ait donnée jusqu'ici du mot de *mathématiques*. Mais, quoique cette définition paraisse embrasser la science tout entière, il me semble qu'elle n'en donne encore une idée ni assez profonde ni assez étendue. Les mathématiques ne sont pas seulement la science des rapports, je veux dire que l'esprit n'y a pas uniquement en vue la *proportion* ou la *mesure*; il peut encore considérer le *nombre* en lui-même, l'*ordre* et la *situation* des choses, sans aucune idée de leurs rapports, ni des distances plus ou moins grandes qui les séparent. Si l'on parcourt les différentes parties des mathématiques, on y trouve partout ces deux objets de nos spéculations.

Ainsi l'Arithmétique nous offre d'abord l'arithmétique ordinaire, qui n'est guère autre chose que l'art de la numération, et qui peut s'établir d'une infinité de manières, selon l'échelle ou la base que l'on veut choisir. Mais les nombres, considérés en eux-mêmes, ont des propriétés qui ne dépendent point du tout de la manière dont on les représente, ou dont on opère actuellement sur eux. Ainsi il y a des nombres

[*] Voyez le volume XIV et dernier de la *Classe des Sciences mathématiques de l'Institut*, et le tome IV des *Mémoires de l'Académie des Sciences*

qui ne peuvent être divisés par aucun autre, et qu'on nomme *premiers*, ou *simples*, parce que tous les autres s'en *composent* par la multiplication; il y a les différentes *puissances* des nombres, qu'on produit en les multipliant plusieurs fois par eux-mêmes; et une foule d'autres formés par diverses lois, et par toutes les combinaisons régulières de celles-là. Or tous ces nombres et leurs propriétés demeurent toujours les mêmes dans tous les systèmes possibles de numération; et de là résulte un certain genre de spéculations et de vérités mathématiques, qui constituent cette arithmétique transcendante qu'on nomme aujourd'hui la *théorie des nombres*.

Si vous considérez l'Algèbre, vous y voyez également deux parties très-distinctes. Et d'abord, l'algèbre ordinaire, qu'on peut très-bien nommer l'*arithmétique universelle*. Cette algèbre, en effet, n'est autre chose qu'une arithmétique généralisée, c'est-à-dire étendue des nombres particuliers à des nombres quelconques, et, par conséquent, des opérations actuelles qu'on exécutait à des opérations qu'on ne fait plus qu'indiquer par des signes; de manière que, dans cette première spéculation de l'esprit, on songe moins à obtenir le résultat de ces opérations successives qu'à en tracer le tableau, et à découvrir ainsi des formules générales pour la solution de tous les problèmes du même genre.

Mais il y a une algèbre supérieure, qui repose tout entière sur la théorie de l'ordre et des combinaisons, qui s'occupe de la nature et de la composition des formules considérées en elles-mêmes, comme de purs symboles, et sans aucune idée de valeur ou de quantité. C'est à cette partie qu'on doit rapporter la théorie profonde des équations, celle des expressions imaginaires, et tout l'art des transformations algébriques; et c'est même cette seule partie élevée de la science qui mérite, à proprement parler, le nom d'*algèbre*.

Si l'on passe maintenant à la Géométrie, qu'on définit la science de l'*étendue figurée*, on y voit d'abord la géométrie ordinaire, qui étudie les propriétés des figures sous le seul point de vue des rapports de grandeur, et qui n'a ainsi d'autre objet que la proportion ou la mesure. Mais on distingue ensuite une autre géométrie, qui ne regarde, pour ainsi dire, que les lieux dans l'espace, c'est-à-dire l'ordre et la situation des choses, sans aucune considération de leur grandeur ou de leur figure. C'est une science encore neuve, que Leibnitz paraît avoir le

premier entrevue, et qu'il a nommée la *géométrie de situation*. Il en avait pris l'idée dans la considération de quelques jeux remarquables, dont la loi ne dépend que de la situation des différentes pièces qu'on y emploie; mais elle s'étend à beaucoup d'autres questions importantes, et c'est à cette géométrie que j'ai cru devoir rapporter les *polygones* et les *polyèdres étoilés*, et plusieurs problèmes d'ordre et de situation que j'ai proposés et résolus pour la première fois dans un Mémoire qui a été imprimé dans le *Recueil de l'Institut* et dans le *Journal de l'École Polytechnique*.

La Mécanique elle-même nous présenterait également deux espèces de mécanique. Et d'abord celle qui calcule la quantité des mouvements, les forces, les vitesses; ensuite celle qui n'a en vue que la disposition des corps, leur jeu réciproque, la manière dont ils croisent leurs routes, et cela sans avoir égard ni à la direction de ces lignes, ni au temps que les corps mettent à les décrire, ni aux forces qui sont nécessaires pour les mouvoir. Telles sont plusieurs machines ou mécaniques ingénieuses, où l'on ne considère ni la force ni la grandeur du mouvement, mais uniquement la situation et le mouvement géométrique des différentes pièces qui les composent. Mais il est clair que cette espèce de mécanique serait toute fondée sur la géométrie de situation, et se confondrait, pour ainsi dire, avec elle.

Quoi qu'il en soit, vous voyez que les mathématiques nous offrent partout ces deux objets de spéculation : d'un côté, la *grandeur* ou la *quantité*, c'est-à-dire la *proportion* ou la *mesure* des grandeurs; de l'autre, le *nombre*, l'*ordre* et la *situation* des choses, sans aucune idée de mesure ou de quantité. De sorte que les mathématiques, considérées de la manière la plus générale, pourraient être définies la science qui a pour objet le *nombre*, l'*ordre* et la *mesure*.

Je mets la théorie des nombres en premier lieu, parce qu'elle est nécessairement la première qui doive s'offrir dans la chaîne naturelle de nos idées, et que la science des rapports y a elle-même ses premiers principes. Et, en effet, il n'est guère de problème mathématique, quelque simple qu'il soit, qui ne présente *plusieurs* choses à considérer, et qui n'ait ainsi de premières difficultés relatives au *nombre* de ces choses; de sorte que les premiers principes de la solution doivent être nécessairement puisés dans la théorie des nombres.

Cependant cette spéculation, que je mets la premiere dans la suite de nos idées, paraît ne s'être présentée que la seconde; et même on a vu les diverses branches des mathématiques s'élever à une assez grande hauteur, sans rien emprunter à la théorie des nombres, qui est restée, pour ainsi dire, isolée, et comme sans usage dans l'analyse et la géométrie. Mais il y a là-dessus une remarque essentielle à faire.

Il faut observer que la plupart des questions traitées jusqu'ici par les géomètres ont exigé, si j'ose le dire, encore plus d'adresse et de sagacité que de force et de profondeur. N'ayant presque jamais en vue que la *quantité,* ils ont pu la saisir, et même la suivre jusque dans les affections des grandeurs qui varient par nuances insensibles. Dans les premiers problèmes qui nous intéressent, il y a si peu d'éléments à considérer, que les difficultés qui tiennent au nombre et à l'ordre de ces éléments disparaissent pour ainsi dire d'elles-mêmes, et ne peuvent guère retarder la solution qu'on se propose d'obtenir. Mais sitôt qu'on a voulu résoudre des questions un peu moins simples, ces difficultés se sont fait sentir, et nous ont paru insurmontables. Dans ces sortes de recherches, on a à peine effleuré la matière; et les solutions particulières, qu'on avait obtenues dans quelques cas simples, n'étant pas tirées des principes généraux, n'ont pu donner aucune lumière sur les questions du même genre. C'est ce qu'on peut voir et rendre sensible par plusieurs exemples, et, entre autres, par cet exemple remarquable que j'ai cité plus haut. Ainsi les Anciens ont trouvé qu'on pouvait construire, par la règle et le compas, le côté du *triangle* équilatéral, et même le côté du *pentagone* régulier, inscrits à un cercle donné; et, quoiqu'ils aient trouvé dans ces deux cas des constructions exactes, ils n'ont rien vu au delà, et ils ont même cru qu'on ne pouvait aller plus loin. Ils ont pu résoudre le probleme pour ces deux nombres premiers 3 et 5, parce que la difficulté qui vient des nombres est ici presque nulle, et n'est pas même aperçue. Mais il n'en est pas de même pour les nombres premiers supérieurs, et ils ont été arrêtés tout à coup dans leur recherche, parce que les vrais principes de la solution, qui ne peuvent être pris que dans la théorie des nombres, leur ont entièrement échappé. Et, en effet, s'ils avaient eu ces principes, ils auraient vu que la possibilité de diviser géométriquement le cercle en 3 ou 5 parties égales tient essentiellement à une propriété qui est commune

à ces deux nombres premiers, et qui consiste en ce que chacun d'eux, étant diminué de l'unité, fait une puissance exacte de 2; et de là ils auraient conclu que la solution est également possible pour les autres nombres premiers, tels que 17, 257, etc., qui jouissent aussi de la même propriété; mais c'est ce que leur solution, trouvée dans le cas de 3 et 5, ne leur avait pas même fait soupçonner, parce que ce n'était, pour ainsi dire, qu'une solution de fait, et qui ne venait pas de cette propriété des nombres, qui seule la fait réussir.

Il résulte donc de ces réflexions que la théorie des nombres, qui, au premier coup d'œil, ne paraît qu'une spéculation singulière en mathématiques, s'y présente au contraire d'une manière naturelle, et qu'elle forme même la première partie essentielle de la doctrine, comme étant celle où la science générale des rapports a elle-même ses premiers fondements. C'est par cette théorie de l'ordre et des nombres qu'on peut connaître la nature propre de l'algèbre, et rendre raison de cette *équivoque,* ou multiplicité de sens, qu'elle attache à ses signes, et qui nous présente souvent plusieurs racines ou solutions différentes dans un problème où notre esprit n'en voit qu'une seule: propriété singulière de l'algèbre, dont on ne s'est point encore bien rendu compte, et que je vais tâcher d'approfondir afin de jeter un nouveau jour sur la philosophie de la science.

III.

Quand on applique l'algèbre à la solution d'un problème, on trouve souvent une équation de degré supérieur, qui a plusieurs racines, et qui donne ainsi, outre la valeur propre à résoudre le problème tel que l'esprit le considère, d'autres valeurs auxquelles on n'avait pas songé, et qu'il paraît quelquefois impossible d'interpréter par les nombres ou par les lignes dont il s'agit dans la question proposée.

D'Alembert a fait là-dessus des réflexions dans plusieurs de ses écrits, et notamment dans le dictionnaire de l'Encyclopédie, au mot *Équation*. Il parcourt quelques questions très-simples, où l'algèbre donne à la fois plusieurs solutions différentes, quoique le problème paraisse n'en avoir qu'une seule dans le sens précis de son énoncé; et il tâche d'expliquer cette multiplicité, en faisant voir que l'équation est souvent

plus générale que l'énoncé, et qu'elle est la traduction algébrique de plusieurs énoncés différents dont l'algèbre ne peut exprimer la différence. « Quelques algébristes, dit-il, regardent cette généralité comme » une richesse de l'algèbre, qui répond, non-seulement à ce qu'on » lui demande, mais encore à ce qu'on ne lui demandait pas et qu'on » ne songeait pas à lui demander.... Pour moi, ajoute d'Alembert, je » ne puis m'empêcher d'avouer que cette richesse prétendue me paraît un inconvénient. Souvent il en résulte qu'une équation monte » à un degré beaucoup plus haut qu'elle ne monterait, si elle ne renfermait que les racines propres à la vraie solution de la question telle » qu'elle est proposée. Il est vrai que cet inconvénient serait moindre, » et serait même, en un sens, une véritable richesse, si l'on avait une » méthode générale pour résoudre les équations de tous les degrés. Il » ne s'agirait plus que de démêler parmi les racines celles dont on » aurait vraiment besoin; mais malheureusement on se trouve arrêté » dès le quatrième degré. Il serait donc à souhaiter, puisqu'on ne peut » résoudre toute équation, qu'on pût au moins l'abaisser au degré de » la question, c'est-à-dire à n'avoir qu'autant d'unités dans l'exposant » de son degré, que la question a de solutions vraies et directes; mais » la nature de l'algèbre ne paraît pas le permettre. »

Telles sont à ce sujet les réflexions de d'Alembert, philosophe à qui l'on doit sans doute beaucoup de lumières sur d'autres points de la science; mais il me semble qu'ici ses réflexions manquent à la fois de force et de justesse, et qu'elles ne vont point au fond de la question philosophique dont il s'agit. Cette généralité de l'algèbre n'est ni une *richesse* ni un *inconvénient :* c'est le simple caractère d'une science exacte et parfaite; car l'algèbre ne nous donne exactement que ce qu'un raisonnement parfait nous aurait donné lui-même.

Supposons, en effet, que le problème dont on s'occupe soit énoncé d'une manière parfaite : l'énoncé ne renfermera que la relation précise qui existe entre l'inconnue et les données du problème, et qui seule forme entre elles une *équation.* Il est clair que tout ce qu'on pourrait ajouter à cet énoncé, ou y sous-entendre, serait au moins inutile, et quelquefois même pourrait être une contradiction. Car, puisque l'inconnue se trouve déjà *fixée* par cette seule partie de l'énoncé qui forme l'équation. il est évident qu'on n'est plus le maître

de rien ajouter; comme, par exemple, cette condition que l'inconnue sera plus grande ou plus petite qu'une certaine quantité, ou que la ligne cherchée tombera dans telle ou telle partie de la figure, etc.; conditions qui ne dépendent plus de nous, que l'esprit peut supposer mal à propos, et qui souvent n'ont pas lieu dans la question proposée. On voit donc que si l'énoncé du problème est parfait, il n'est rien autre chose que l'équation même qui le traduit en algèbre. Si donc cette équation nous présente plusieurs racines ou valeurs différentes de l'inconnue, l'énoncé lui-même doit également présenter, à l'esprit attentif, cette même multiplicité de solutions dans le problème dont il s'agit.

L'algèbre ne donne donc rien au delà de ce qu'on lui demande; elle n'est pas plus générale que la logique considérée dans sa perfection, et le degré où l'équation s'élève est le degré même de la question, si elle parfaitement posée.

Mais le plus souvent nos énoncés sont très-imparfaits; je veux dire, qu'indépendamment de cette relation qui lie aux données l'inconnue et qui la *détermine,* notre esprit y mêle encore certaines conditions inutiles et souvent contradictoires; et voici alors ce qui nous arrive. Comme ces sortes de restrictions ne donnent point d'équation, et ne sont pas ainsi de nature à s'écrire en algèbre, l'équation qu'on tire de l'énoncé se trouve exactement la même que si ces suppositions n'avaient point lieu, et, par conséquent, cette équation a les mêmes racines ou solutions différentes dont le problème est susceptible en le supposant bien exprimé. Cependant, comme notre esprit reste toujours préoccupé par la considération particulière de ces limites où il borne la question, il s'étonne d'abord de cette multiplicité de solutions qu'il n'avait point en vue, et il cherche ensuite à les interpréter par les lignes, ou par les quantités dont il s'agit dans la question proposée. S'il en vient à bout, il attribue à l'algèbre, qui lui a donné ces solutions inattendues, une généralité propre qu'il n'avait pas trouvée dans le raisonnement ordinaire; s'il ne peut expliquer toutes ces valeurs, il reproche à l'algèbre cette trop grande généralité, comme un inconvénient, et une imperfection qui mêle la vraie valeur de l'inconnue à des valeurs étrangères. Mais on voit qu'il n'y a ici d'autre imperfection que celle de l'esprit et du langage. L'algèbre, encore une fois, ne

traduit et ne doit traduire, de l'énoncé du problème, que la seule partie qui fait une *équation,* et qui suffit pour *déterminer* l'inconnue. Elle abandonne tout le reste, comme ces rapports vagues de *majorité* ou de *minorité,* qui ne peuvent servir à aucune *détermination.* Ainsi l'équation obtenue ne renferme rien des imperfections de notre énoncé, et elle devient la question même parfaitement posée. La multiplicité de ses racines nous avertit donc, non pas, comme on le croit d'ordinaire, qu'il faut *étendre* le premier énoncé pour en multiplier les *divers sens;* mais qu'il faut, au contraire, le simplifier et le *réduire,* en y supprimant ce qu'on y avait mis de trop et qu'on n'était pas le maître d'y insérer. Et alors on peut voir qu'il n'y a précisément, dans l'équation algébrique, que la même multiplicité de solutions qu'on aurait pu reconnaître, sans algèbre, dans l'énoncé parfait du problème.

Telle est, je crois, la vraie nature de l'algèbre, et la vraie solution de la question philosophique que j'examine, et qui touche aux premiers fondements de la science mathématique. Il ne s'agit pas de savoir s'il y a, ou non, une méthode générale pour résoudre les équations de tous les degrés : on n'en sait pas moins qu'une équation de degré supérieur a plusieurs racines, et la question était d'expliquer cette multiplicité, en montrant qu'elle est dans la nature même des choses, et que l'algèbre n'a pas plus de généralité qu'un bon raisonnement.

Mais il ne faut pas manquer de faire ici une observation essentielle : c'est que, à raison de l'ignorance et de la faiblesse de l'esprit humain, qui ne marche guère qu'à l'aide des images sensibles, ou des mots qui eux-mêmes ne répondent presque tous qu'à des images, l'algèbre nous a été et nous est encore d'un merveilleux secours. Car, comme elle n'exprime que les rapports qui *déterminent,* et qu'elle n'a point de signes pour les conditions vagues, il en résulte que, quelque imparfaits que soient nos énoncés, pourvu qu'ils renferment la loi de rapport qui fait le nœud du problème, l'équation que l'analyse en tire se trouve aussi parfaite que si elle provenait de l'énoncé le plus parfait ; et, sous ce point de vue, on peut dire que l'algèbre a étendu et perfectionné l'esprit humain.

On voit donc que ce qui nous resterait à faire aujourd'hui pour l'achèvement de la doctrine, ce serait de chercher et de montrer dans chaque problème comment l'esprit, à l'aide du seul raisonnement, au-

rait pu s'élever à cette généralité de vue dont il n'a été averti que par les signes de l'algèbre, et comment il aurait dû prévoir ces multiples solutions qui coexistent dans un même problème, et qu'aucun art ne peut séparer. C'est par cette étude attentive qu'il verra ce qui avait manqué jusqu'ici aux principes de son analyse logique. Il n'avait songé qu'aux rapports de grandeur, et il reconnaîtra qu'il fallait avant tout considérer le nombre et l'ordre des choses, indépendamment de toute idée de grandeur ou de quantité. Dans cette pure considération de l'ordre, où il verra que plusieurs ordres, qui lui paraissent différents, naissent pourtant l'un de l'autre par une seule et même loi, et se reproduisent sans cesse, quel que soit le premier ordre d'où l'on veuille partir, il trouvera l'origine naturelle des *puissances*, et la raison profonde de ces *multiples racines* de l'unité, qui ne sont point des *valeurs*, mais de simples *signes d'ordre* entre les choses que l'on considère. Par ces nouveaux principes il perfectionnera l'algèbre elle-même, et l'algèbre à son tour pourra jeter de nouvelles lumières sur la théorie des nombres.

De toutes ces réflexions, et d'une foule d'autres que je pourrais y ajouter, je conclus donc que les principes de l'algèbre et de la théorie des nombres devraient être unis ensemble dans nos ouvrages élémentaires, comme ils sont inséparables par la nature même de ces deux sciences. Ainsi j'espère qu'on me pardonnera, et même qu'on me saura quelque gré de revenir sur ces principes fondamentaux, d'essayer de les rendre plus clairs et plus sensibles, et de faciliter ainsi aux jeunes géomètres une étude très-ardue, et en apparence très-stérile, mais en effet très-féconde, et peut-être, comme je l'ai dit, la seule d'où l'analyse mathématique puisse attendre aujourd'hui de véritables découvertes.

CHAPITRE Ier.

De quelques propositions fondamentales de la théorie des nombres.

Je commencerai par établir le théorème général qui regarde le nombre des racines ou solutions entières d'une équation indéterminée de degré quelconque. Ce théorème est tout à fait analogue à celui qui sert de base en algèbre à la théorie générale des équations, et je vais

les démontrer tous deux de la même manière. J'examinerai ensuite les autres théorèmes à mesure qu'ils se présenteront dans le cours naturel de ces réflexions.

Article Ier.

Sur le nombre des entiers qui peuvent rendre un polynôme divisible exactement par un nombre premier.

1. Considérez un polynôme rationnel et entier du degré m, de la forme

$$x^m + Ax^{m-1} + Bx^{m-2} + \cdots + Sx + T,$$

et que, pour abréger, je désignerai par X. Prenez m quantités quelconques $a, b, c, \ldots, s, t$, et divisez le polynôme X par le binôme $x-a$, jusqu'à ce que le reste ne contienne plus la lettre x, ce qui est toujours possible; vous aurez l'équation

$$X = (x-a)X' + X_a,$$

le quotient X' étant un polynôme du degré $m-1$ en x, et le reste X_a étant le polynôme proposé X où l'on aurait changé x en a.

Divisez de même X' par $x-b$ et vous aurez de la même manière un quotient X'' du degré $m-2$, et un reste X'_b qui sera le polynôme X' où l'on aurait changé x en b; et par conséquent vous aurez

$$X' = (x-b)X'' + X'_b.$$

Continuez de même de diviser X'' par $x-c$, et ainsi de suite jusqu'au dernier polynôme X^{m-1} qui ne sera plus que du premier degré en x, et que vous diviserez par $x-t$; et vous trouverez enfin

$$X^{m-1} = (x-t) + X_t^{m-1}.$$

Substituez maintenant dans la première équation, à la place de X', sa valeur donnée par la seconde, et dans l'équation résultante, à la place de X'', sa valeur donnée par la troisième, et ainsi de suite; et vous aurez l'équation

$$X = X_a + (x-a)X'_b + (x-a)(x-b)X''_c + (x-a)(x-b)(x-c)X'''_d + \cdots$$
$$+ (x-a)(x-b)(x-c)\cdots(x-s)(x-t);$$

équation *identique*, c'est-à-dire, qui *aura lieu quelles que soient les quantités que vous vouliez prendre pour* $a, b, c, \ldots, s, t$.

2. Or actuellement supposons que la quantité désignée par a soit telle qu'étant mise au lieu de x dans le polynôme proposé, elle réduise ce polynôme X à zéro; alors le terme marqué par X_a sera nul de lui-même, et l'équation précédente se réduira à celle-ci :

$$X = (x-a)X'_b + (x-a)(x-b)X''_c + (x-a)(x-b)(x-c)X'''_d + \cdots + (x-a)(x-b)(x-c)\ldots(x-s)(x-t).$$

Supposons ensuite que b soit aussi une quantité capable de réduire X à zéro; on aurait donc $X_b = 0$; mais l'équation précédente, en faisant $x = b$, donnerait $X_b = (b-a)X'_b$; donc si b diffère de a, $X_b = 0$ donne nécessairement $X'_b = 0$, et la transformée se réduit encore et devient ainsi

$$X = (x-a)(x-b)X''_c + (x-a)(x-b)(x-c)X'''_d + \cdots + (x-a)(x-b)(x-c)\cdots(x-s)(x-t).$$

De même, si $x = c$ rend nul le polynôme X, on aura $X''_c = 0$, et ainsi de suite; de sorte que *si* $a, b, c, \ldots, s, t$ *sont* m *quantités qui puissent réduire le polynôme* X *à zéro, ce polynôme peut être transformé identiquement dans le produit*

$$(x-a)(x-b)(x-c)\cdots(x-s)(x-t);$$

ce qui est le fondement de toute la théorie des équations.

3. On voit par là qu'il n'y a pas plus de manières de réduire à zéro le polynôme X du degré m, qu'il n'y a de manières de réduire à zéro le produit de m facteurs $x-a$, $x-b$, $x-c, \ldots$, $x-s$, $x-t$; or il est évident qu'un produit ne peut jamais devenir nul à moins que quelqu'un de ses facteurs ne soit nul en particulier; de plus, chaque facteur $x-a$ ne peut devenir nul que d'une seule manière, savoir, en faisant $x = a$; *donc un polynôme* X *du degré* m *ne peut devenir nul pour plus de* m *valeurs de* x, *c'est-à-dire que l'équation* $X = 0$ *ne peut avoir plusde racines qu'il n'y a d'unités dans le degré de cette équation.*

4. Soit maintenant p un nombre premier quelconque, et considé-

rons les nombres entiers x inférieurs à p, qui peuvent rendre le polynôme X divisible par p : ces nombres entiers seront les solutions ou *racines* de l'équation indéterminée $X = \mathfrak{M}p$, en désignant par $\mathfrak{M}p$ un multiple quelconque de p ; et je dis que cette équation ne peut avoir plus de racines qu'il n'y a d'unités dans le degré m de cette proposée.

En effet, si nous reprenons l'équation identique

$$X = X_a + (x-a)X'_b + (x-a)(x-b)X''_c + (x-a)(x-b)(x-c)X'''_d + \cdots + (x-a)(x-b)(x-c)\cdots(x-s)(x-t),$$

nous voyons qu'en supposant a un nombre inférieur à p, qui rende X divisible par p, de manière qu'on ait $X_a = \mathfrak{M}p$, le polynôme X devient, à ce multiple près de p,

$$X = (x-a)X'_b + (x-a)(x-b)X'' + (x-a)(x-b)(x-c)X'''_d + \cdots + (x-a)(x-b)(x-c)\cdots(x-s)(x-t).$$

De même, si $x = b$ rend X divisible par p, de manière qu'on ait $X_b = \mathfrak{M}p$, comme l'équation précédente donne $X_b = (b-a)X'_b$, il en résulte qu'on aurait $(b-a)X'_b = \mathfrak{M}p$; mais b et a étant des nombres différents inférieurs à p, il est clair que le facteur $b-a$ ne peut être divisible par p; donc l'autre facteur X'_b doit l'être; donc $X_b = \mathfrak{M}p$ donne nécessairement $X'_b = \mathfrak{M}p$, et le polynôme X, à un multiple près du nombre p, se réduit à

$$X = (x-a)(x-b)X''_c + (x-a)(x-b)(x-c)X'''_d + \cdots + (x-a)(x-b)(x-c)\cdots(x-s)(x-t).$$

De même, si le nombre $x = c$ rend X divisible par p, on en conclura $X''_c = \mathfrak{M}p$, et ainsi de suite; de sorte que *si $a, b, c, \ldots, s, t$ sont m nombres entiers inférieurs à p qui rendent* X *divisible par p, ce polynôme* X *du degré m sera, à des multiples près du nombre p, équivalent au produit des m facteurs binômes $x-a$, $x-b$, $x-c, \ldots, x-s$, $x-t$.* Ainsi il n'y aura pas plus de manières de rendre le polynôme divisible par p qu'il n'y en a pour le produit équivalent dont il s'agit.

Or, p étant un nombre premier, ce produit ne peut devenir divisible par p, qu'autant que l'un des facteurs le sera séparément; mais il est évident que chacun d'eux, tel que $x - a$, ne peut l'être que pour une

seule valeur de x inférieure à p, savoir, $x = a$; *donc l'équation indéterminée* $X = \mathfrak{M}p$, *du degré* m, *ne peut avoir plus de* m *racines ou solutions en nombres entiers inférieurs à* p.

Remarque I.

5. J'ai supposé tout de suite que le premier terme x^m de la proposée n'avait pour coefficient que l'unité, parce qu'il est aisé de voir qu'on peut toujours réduire à cette forme une équation quelconque

$$Ax^m + Bx^{m-1} + Cx^{m-2} + \cdots + Sx + T = \mathfrak{M}p,$$

en ajoutant aux coefficients B, C,..., T, des multiples convenables de p, qui les rendent tous divisibles par le premier coefficient A que je suppose premier à p. Il est évident que ces multiples de p ajoutés aux coefficients ne peuvent changer en rien les racines de la proposée, mais ils rendent tout le premier membre divisible par A, et l'on a la transformée

$$x^m + A'x^{m-1} + B'x^{m-2} + \cdots + S'x + T' = \mathfrak{M}p,$$

qui a les mêmes racines et dont le premier terme n'a d'autre coefficient que l'unité.

Si A n'était pas premier à p, il serait donc de la forme μp et l'on pourrait alors supprimer le premier terme de l'équation, laquelle ne serait ainsi que du degré $m - 1$; et de même pour le coefficient suivant B, s'il n'était pas premier à p.

Si tous les coefficients A, B, C,..., S, T étaient divisibles par p, le polynôme proposé serait toujours divisible par p pour toutes les valeurs possibles de x, ou, pour mieux dire, il n'y aurait plus alors d'équation.

6. Quant à ce multiple convenable de p qu'il faut ajouter à un coefficient B, pour le rendre divisible par A, on le trouve facilement en posant l'équation du premier degré,

$$\frac{B + ip}{A} = \text{un entier} = e,$$

ou

$$eA - ip = B,$$

équation toujours possible si A est premier à p, et qui fera connaître les valeurs de i et de e par la méthode connue [*]. On opérerait de la même manière pour rendre tous les autres coefficients C, D,..., S, T divisibles par A. Ces transformations sont tout à fait analogues à celles qu'on emploie dans les équations algébriques pour faire disparaître les fractions et réduire le premier coefficient à l'unité.

Ainsi nous considérerons toujours les équations indéterminées sous cette forme très-simple, où le premier coefficient est 1, et tous les autres réduits à des entiers, comme nous l'avons supposé dans la démonstration du théorème fondamental que nous venons de présenter (n° 4).

Remarque II.

7. Lagrange est, comme on sait, le premier qui ait proposé et démontré ce théorème, dans les *Mémoires de l'Académie de Berlin* pour l'année 1768. Euler, dans le tome XVIII des *Nouveaux Commentaires de Saint-Pétersbourg*, l'a démontré dans le cas de l'équation binôme, mais par une méthode qu'il est facile d'étendre à une équation quelconque. On le trouve encore dans les Recherches de Legendre sur l'analyse indéterminée, dans sa *Théorie des nombres*, et dans l'ouvrage de M. Gauss. Mais toutes ces démonstrations sont à peu près la même, présentée de différentes manières : la nôtre nous paraît aussi claire et aussi simple qu'on puisse le désirer.

Remarque III.

8. Cette démonstration suppose essentiellement que le nombre ou *module* p auquel on rapporte l'équation soit un nombre premier. Car s'il s'agissait d'un module composé N, le produit des binômes $x - a$, $x - b$, $x - c$,... pourrait être encore divisible par N sans qu'aucun d'eux le fût séparément. Il suffirait que l'un de ces binômes fût divisible par un des facteurs de N, et un autre par l'autre facteur, et le produit serait encore divisible par N ; d'où l'on voit que l'équation

[*] On donnera plus loin quelques méthodes nouvelles pour résoudre les équations indéterminées du premier degré.

$X = \mathfrak{M}N$ peut avoir, si N est un nombre composé, plus de racines qu'il n'y a d'unités dans l'exposant de son degré. Il serait facile de compter le nombre de toutes les solutions possibles, par le nombre de toutes les manières possibles de décomposer le nombre N en différents facteurs premiers entre eux; mais nous y reviendrons, et nous ne considérerons ici que le cas d'un module absolument premier et que nous désignerons toujours par la même lettre p.

Remarque IV.

9. On peut remarquer encore que cette démonstration sur le nombre des racines entières de l'équation indéterminée $X = \mathfrak{M}p$, est tout à fait la même que la démonstration relative au nombre des racines des équations déterminées $X = 0$. On n'y suppose absolument que l'opération de la division algébrique, et ce théorème fondamental, démontré par Euclide, que si deux nombres sont premiers par rapport à un troisième, leur produit est aussi premier à ce troisième nombre. Il résulte donc des premiers principes du calcul qu'une équation indéterminée du degré m,

$$x^m + Ax^{m-1} + Bx^{m-2} + \cdots = \mathfrak{M}p,$$

ne peut avoir plus de m racines ou solutions en nombres entiers inférieurs à p; car une fois qu'on lui en supposerait m, on prouverait tout de suite qu'elle est, aux multiples près de p, identique avec l'équation

$$(x - a)(x - b)(x - c)\cdots = \mathfrak{M}p,$$

laquelle ne peut avoir d'autres racines que a, b, c, etc. Par la même démonstration on voit encore qu'une équation $X = \mathfrak{M}p$, du degré m, peut avoir autant de racines qu'il y a d'unités dans l'exposant m de ce degré; car on peut sur-le-champ former une équation

$$x^m + Ax^{m-1} + \cdots = \mathfrak{M}p,$$

qui aurait m racines données a, b, c, etc.: il n'y aurait qu'à faire le produit $(x - a)(x - b)(x - c)\ldots$ et à l'égaler à un multiple quelconque de p. Ainsi il y a une infinité d'équations

$$x^m + Ax^{m-1} + \cdots = \mathfrak{M}p,$$

qui ont effectivement m racines, et il ne peut y en avoir aucune du degré m qui ait plus de m racines; mais voilà tout ce qui résulte de la démonstration précédente. Lorsqu'on propose une équation du degré m, on ne peut savoir en général si elle a ou non des solutions en nombres entiers. Il n'y a qu'un cas particulier, fort remarquable, où l'on connaisse toujours le nombre et les valeurs des racines par la forme même de l'équation proposée; c'est le cas de l'équation binôme $x^{p-1} - 1 = \mathfrak{M}p$, laquelle a toujours pour racines les $p - 1$ nombres entiers $1, 2, 3, 4, 5, \ldots, p - 1$, inférieurs à p : ce qui est, en d'autres termes, l'expression du fameux théorème de Fermat.

Corollaire.

10. Mais, de ce théorème, qui sera démontré plus loin, on peut tirer une conséquence générale sur le nombre des racines entières que peut admettre une équation quelconque

$$x^m + Ax^{m-1} + Bx^{m-2} + \cdots = \mathfrak{M}p.$$

Car puisque, aux multiples près de p, le binôme $x^{p-1} - 1$ est identique avec le produit

$$(x-1)(x-2)(x-3)\cdots(x-\overline{p-1}),$$

il en résulte que, si la proposée

$$x^m + Ax^{m-1} + \cdots = \mathfrak{M}p$$

a m racines entières, e, e', e'', etc., inférieures à p, le premier membre $x^m + Ax^{m-1} + \ldots$ est nécessairement un diviseur du binôme $x^{p-1} - 1$; ou plus généralement, que si elle a un nombre θ de racines entières, le polynôme $x^m + Ax^{m-1} + \ldots$ aura nécessairement avec $x^{p-1} - 1$ un commun diviseur du degré θ, et la réciproque est manifeste. D'où je conclus qu'on pourra toujours reconnaître si une proposée

$$x^m + Ax^{m-1} + \cdots = \mathfrak{M}p$$

a des racines entières, et quel est le nombre de ces racines, en cherchant le plus grand commun diviseur du polynôme $x^m + Ax^{m-1} + \ldots$ et du binôme $x^{p-1} - 1$. Si ce commun diviseur existe, et qu'il soit du

degré θ, la proposée aura θ racines entières; s'il n'y a pas de commun diviseur, la proposée n'admettra aucune racine entière. On voit donc que toutes les équations

$$x^m + Ax^{m-1} + \ldots = \mathfrak{M}p,$$

qui admettent m racines, ne sont, aux multiples près de la base ou module p, que des diviseurs de l'équation binôme $x^{p-1} - 1 = \mathfrak{M}p$; et qu'ainsi cette équation, qui semblait particulière, est au fond très-générale et renferme en quelque sorte toutes les autres; ce qui fait sentir d'abord toute l'importance du théorème de Fermat dans l'analyse indéterminée.

Article II.

Sur le théorème de Fermat.

11. Ce théorème a été démontré pour la première fois par Euler, et depuis par presque tous ceux qui se sont occupés des propriétés des nombres. J'en proposerai encore dans ce Mémoire deux démonstrations nouvelles extrêmement simples. Mais, auparavant, je suis bien aise d'indiquer celle que Lagrange en a donnée dans les *Mémoires de Berlin* pour l'année 1771, et qui paraît assez naturellement déduite des premiers principes du calcul.

12. Cet illustre auteur fait voir que, si l'on forme l'équation

$$(x-1)(x-2)(x-3)(x-4)(x-5)\cdots(x-\overline{p-1}) = 0,$$

p étant un nombre premier, et qu'on représente le polynôme qui en résulte par

$$x^{p-1} + Ax^{p-2} + Bx^{p-3} + \cdots + T - 1 = 0,$$

tous les coefficients A, B, C, etc., T, seront divisibles par le nombre premier p.

Ainsi tous les coefficients peuvent être représentés par αp, βp, γp, etc., τp; de sorte que l'équation qui a pour racines les nombres 1, 2, 3, 4, 5,..., $p-1$, est de cette forme

$$x^{p-1} + \alpha p x^{p-2} + \beta p x^{p-3} + \cdots + \tau p - 1 = 0.$$

Or, par la théorie des équations, on sait que le dernier terme $\tau p - 1$ est égal au produit de toutes les racines 1, 2, 3, 4, 5,..., $p-1$; ainsi l'on a

$$1.2.3.4.5...\overline{p-1} = \tau p - 1,$$

ou

$$1.2.3.4.5...\overline{p-1} + 1 = \tau p,$$

et par conséquent *le produit de tous les nombres* 1, 2, 3, 4, 5,..., $\overline{p-1}$, *augmenté de l'unité, est toujours divisible par p, quand p est un nombre premier :* ce qui donne d'abord le beau théorème qu'on attribue à Wilson, et que personne n'avait encore démontré.

Ensuite la même équation précédente, mise sous la forme

$$x^{p-1} - 1 = -(\alpha x^{p-2} + 6x^{p-3} + \text{etc.} + \tau)p,$$

fait voir que le binôme $x^{p-1} - 1$ est toujours divisible par p, quelque valeur 1, 2, 3, 4, 5,..., $p-1$, qu'on veuille donner à x.

Donc l'équation indéterminée $x^{p-1} - 1 = \mathfrak{M}p$ a toujours $p-1$ racines ou solutions entières, qui sont 1, 2, 3, 4, 5, etc., $p-1$, ou, si l'on veut, $\mu p + 1$, $\mu p + 2$, $\mu p + 3$, $\mu p + 4$, etc., $\mu p + p - 1$: car, en négligeant les multiples de p, une puissance quelconque de $\mu p + e$ revient à la même puissance de e.

Ainsi *le binôme* $x^{p-1} - 1$, *où p est un nombre premier, est toujours divisible par p, en prenant pour x un nombre quelconque premier à p.* C'est le fameux théorème de Fermat.

13. On déduirait encore de cette même équation,

$$(x-1)(x-2)(x-3)...(x-\overline{p-1}) = x^{p-1} + \alpha p x^{p-2} + \cdots + \tau p - 1,$$

que la somme de tous les nombres

$$1, 2, 3, 4, 5,..., p-1,$$

la somme de leurs produits deux à deux, la somme de leurs produits trois à trois, etc., sont divisibles par p, lorsque p est un nombre premier.

Ainsi le théorème de Fermat, le théorème de Wilson et ceux qu'on vient d'ajouter, sont des corollaires d'une même équation qu'on démontre assez facilement par la méthode des coefficients indéterminés, et par la considération des coefficients du binôme ou des

termes p, $\frac{p.\overline{p-1}}{2}$, $\frac{p.\overline{p-1}.\overline{p-2}}{2.3}$, etc., qui, lorsque p est premier, sont tous entiers, et divisibles par p, à l'exception du dernier $\frac{p.\overline{p-1}.\overline{p-2}\ldots 1}{1.2.3\ldots p}$, qui est égal à l'unité.

Article III.

Théorème de Fermat généralisé.

14. Au reste, le théorème de Fermat peut être en quelque sorte généralisé, c'est-à-dire étendu à un nombre quelconque N, premier ou composé, et s'exprimer de la manière suivante :

Si n *marque combien il* y *a de nombres inférieurs et premiers à* N, *on a toujours* $x^n - 1$ *divisible par* N, *ou* $x^n - 1 = \mathfrak{M}N$, *pourvu que* x *soit un nombre premier à* N.

Ce théorème a été démontré assez directement par Euler dans les *Nouveaux Commentaires de Saint-Pétersbourg* (années 1760 et 1761).

Si le nombre N est premier, alors il est clair que n est égal à $N - 1$, et l'on peut prendre pour x tel nombre qu'on voudra qui ne soit pas un multiple de N ; et ce cas revient exactement au théorème de Fermat.

15. En général, l'équation $x^n - 1 = \mathfrak{M}N$ a n racines entières qui sont les n nombres inférieurs et premiers à N; et il est aisé de voir qu'elle n'en peut avoir d'autres. Car soit, s'il est possible, une racine x qui aurait avec N un commun diviseur θ, de manière qu'on eût

$$x = \theta y \quad \text{et} \quad N = \theta P;$$

on aurait donc, par hypothèse,

$$\theta^n.y^n - 1 = \mathfrak{M}(\theta P),$$

d'où il résulterait

$$\theta^{n-1}.y^n - \frac{1}{\theta} = \mathfrak{M}P,$$

équation impossible, à moins que θ ne soit égal à l'unité, et que, par conséquent, x et N ne soient premiers entre eux. Ainsi l'équation $x^n - 1 = \mathfrak{M}N$ ne peut être résolue que par les nombres premiers à N, et n'a que n racines en nombres entiers inférieurs à N. Quant aux

autres solutions en nombres supérieurs à N, nous ne les considérerons point, puisque, rabaissées au-dessous de N par la division, elles reviendraient aux premières que nous désignerons généralement par

$$1, a, b, c, \text{etc.}, N - 1.$$

Remarque I.

16. Ce qu'on vient de dire est d'autant plus remarquable que si le binôme $x^n - 1$ est résoluble en facteurs rationnels de degrés inférieurs, quelques-uns de ces facteurs, étant séparément égalés à un multiple de N, peuvent avoir plus de solutions qu'il n'y a d'unités dans le plus haut exposant de l'inconnue x, ce qui ne peut jamais arriver quand N est un nombre premier.

Mais dans le cas de N nombre composé, si quelque facteur de $x^n - 1$ égalé à un multiple de N a plus de solutions qu'il n'y a d'unités dans l'exposant, les autres facteurs en auront nécessairement moins, puisque la proposée $x^n - 1 = \mathfrak{M}N$ ne peut avoir en tout plus de n racines.

17. Pour éclaircir la chose par un exemple, considérons le nombre $N = 15$, on aura

$$1,\ 2,\ 4,\ 7,\ 8,\ 11,\ 13,\ 14$$

pour les huit nombres inférieurs et premiers à 15; par conséquent $n = 8$, et l'on a l'équation

$$x^8 - 1 = \mathfrak{M}15;$$

mais le binôme $x^8 - 1$ se décompose de cette manière :

$$(x^2 - 1)(x^2 + 1)(x^4 + 1);$$

or, pour le premier facteur $x^2 - 1$ qui n'est que du second degré, il y a quatre manières de le rendre divisible par 15, savoir, en faisant

$$x = 1, \quad \text{ou} \quad x = 14, \quad \text{ou} \quad x = 4, \quad \text{ou} \quad x = 11.$$

Le second facteur $x^2 + 1$ ne peut être rendu divisible par 15 d'aucune

manière, ni le troisième facteur x^4+1, de sorte que les équations

$$x^2+1=\mathfrak{M}15 \quad \text{et} \quad x^4+1=\mathfrak{M}15$$

ne peuvent avoir aucune solution; mais l'équation résultante du produit des deux premiers facteurs, savoir,

$$(x^2-1)(x^2+1)=x^4-1=\mathfrak{M}15,$$

a encore les quatre solutions

$$2,\ 7,\ 8,\ 13,$$

parce que chacun de ces nombres rend le premier facteur divisible par 3, le second par 5, et par conséquent le produit, divisible par 3.5 ou 15; ainsi l'équation $x^4-1=\mathfrak{M}15$ a les mêmes huit solutions que l'équation $x^8-1=\mathfrak{M}15$; et le facteur x^4+1, égalé à un multiple de 15, n'en a aucune.

Voici le résultat de la substitution des différents nombres premiers à 15, dans le produit des trois facteurs

$$(x^2-1)(x^2+1)(x^4+1)=x^8-1;$$

$$\begin{array}{ll} x=1 \text{ donne} & (0)\ (2)\ (3) = 0.15, \\ x=4 \text{ donne} & (3.5)\ (17)\ (257) = \mathfrak{M}15, \\ x=11 \text{ donne} & (3.5.2^3)(2.61)(2.7321) = \mathfrak{M}15, \\ x=14 \text{ donne} & (3.5.13)(197)(41.937) = \mathfrak{M}15, \end{array}$$

où l'on voit que ces quatre nombres x rendent le seul premier facteur x^2-1 divisible par 15.

Ensuite

$$\begin{array}{ll} x=2 \text{ donne} & (3)\ (5)\ (17) = \mathfrak{M}15, \\ x=7 \text{ donne} & (3.2^4)\ (5^2.2)\ (2.1201) = \mathfrak{M}15, \\ x=8 \text{ donne} & (3^2.7)\ (5.13)\ (17.241) = \mathfrak{M}15, \\ x=13 \text{ donne} & (3.2^2.7)(5.2.17)(2.7^2.17) = \mathfrak{M}15, \end{array}$$

où l'on voit que ces quatre nouveaux nombres x rendent le premier facteur x^2-1 divisible par 3, et en même temps le second x^2+1 divisible par 5; mais le troisième facteur x^4+1 n'est rendu divisible ni par 3 ni par 5, par aucun des huit nombres inférieurs et premiers

à 15, et par conséquent ne peut le devenir par aucun nombre possible; de sorte que l'équation $x^4 + 1 = \mathfrak{M}15$ n'a aucune solution en nombres entiers.

Remarque II.

18. Quand N est un nombre premier p, l'équation $x^n - 1 = \mathfrak{M}N$ devient $x^{p-1} - 1 = \mathfrak{M}p$, et si l'on décompose le premier membre $x^{p-1} - 1$ en différents facteurs rationnels, chacun d'eux égalé à un multiple de p a toujours autant de racines qu'il y a d'unités dans le degré de ce facteur, et n'en a ni plus ni moins. Cela tient à ce que le nombre p étant premier, un produit ne peut jamais être divisible par p, à moins que quelqu'un des facteurs ne le soit séparément. Or un facteur ($x^\theta +$), du binôme proposé, ne peut devenir divisible par p, pour plus de θ valeurs de x, comme on l'a démontré; d'un autre côté, il ne peut l'être pour moins de θ valeurs, car il faudrait alors, ce qui est impossible, que l'autre facteur, qui est du degré $p - 1 - \theta$, le fût pour plus de $p - 1 - \theta$ valeurs, afin qu'on retrouvât les $p - 1$ racines entières qui satisfont toujours à la proposée.

19. Ainsi *l'on a toujours, non-seulement l'équation* $x^{p-1} - 1 = \mathfrak{M}p$ *qui a* $p - 1$ *racines entières, mais encore les équations* $x^\theta - 1 = \mathfrak{M}p$ *qui en ont précisément* θ, *quand* θ *est une aliquote de* $p - 1$: car, dans ce cas, il est clair que $x^\theta - 1$ est un diviseur rationnel de $x^{p-1} - 1$. Mais nous reviendrons avec détail sur la théorie de ces équations.

Auparavant, je veux montrer que le théorème de Wilson peut être aussi généralisé, ou étendu d'un nombre premier p à un nombre quelconque N, et démontré directement de la manière suivante.

Article IV.

Théorème de Wilson généralisé.

20. Soient $1, a, b, c, d$, etc., $N - 1$ les nombres inférieurs et premiers à un nombre quelconque N, il est clair que ces mêmes nombres pourront être mis sous la forme

$$\frac{1 + \mathfrak{M}N}{a}, \quad \frac{1 + \mathfrak{M}N}{b}, \quad \frac{1 + \mathfrak{M}N}{c}, \quad \text{etc.},$$

de manière qu'on aura

$$\frac{1+\mathfrak{M}N}{a}=\alpha,\quad \frac{1+\mathfrak{M}N}{b}=6,\quad \text{etc.},\quad \frac{1+\mathfrak{M}N}{N-1}=N-1,$$

α, 6, etc., étant les mêmes que a, b, etc., mais en général dans un autre ordre, excepté pour le dernier qui, dans tous les cas, donnera toujours

$$\frac{1+\mathfrak{M}N}{N-1}=N-1;$$

on aura donc toujours, quel que soit N,

$$\frac{1+\mathfrak{M}N}{a}\cdot\frac{1+\mathfrak{M}N}{b}\cdot\frac{1+\mathfrak{M}N}{c}\cdots\frac{1+\mathfrak{M}N}{N-1}=\alpha 6\gamma\ldots\overline{N-1}=abc\ldots\overline{N-1},$$

d'où l'on tire (en multipliant les deux membres par $abc\ldots\overline{N-1}$, et réduisant le premier membre à la forme $1+\mathfrak{M}N$), l'équation

$$1+\mathfrak{M}N=(abc\ldots\overline{N-1})^2,$$

ou bien

$$(abc\ldots N-1)^2-1=\mathfrak{M}N.$$

c'est-à-dire que *le carré du produit de tous les nombres inférieurs et premiers à un nombre quelconque* N, *étant diminué de l'unité, est toujours divisible par* N, théorème général qui s'étend à tous les nombres N, simples ou composés.

21. Mais il y a plus: l'équation précédente peut se mettre sous la forme

$$\{(abc\ldots\overline{N-1})+1\}\{(abc\ldots\overline{N-1})-1\}=\mathfrak{M}N,$$

et l'on peut démontrer que l'un ou l'autre des facteurs qui forment le premier membre est séparément divisible par N; et l'on peut distinguer ainsi tous les nombres N en deux classes qui appartiennent à l'un ou à l'autre de ces deux cas. Ceci mérite d'être examiné avec soin.

Je reprends les expressions précédentes,

$$\frac{1+\mathfrak{M}N}{a}=\alpha,\quad \frac{1+\mathfrak{M}N}{b}=6,\quad \text{etc.},\quad \frac{1+\mathfrak{M}N}{N-1}=N-1;$$

et j'observe que si α était toujours différent de a; β différent de b, etc., de manière qu'on eût, par exemple,

$$\frac{1+\mathfrak{M}N}{a}=b,$$

et puis, en prenant un nouveau nombre c,

$$\frac{1+\mathfrak{M}N}{c}=d,$$

et ainsi des autres, il suffirait de considérer la moitié de ces expressions pour voir dans le produit tous les nombres différents a, b, c, etc., de sorte qu'on aurait

$$abcd\ldots=1+\mathfrak{M}N,$$

et multipliant de part et d'autre par $N-1$, il en résulterait

$$abcd\ldots\overline{N-1}=-1+\mathfrak{M}N.$$

Mais s'il arrivait qu'un des nombres α fût égal au nombre a, de manière qu'on eût

$$1+\mathfrak{M}N=a^2,$$

la conclusion précédente ne pourrait plus avoir lieu. Mais alors, au lieu de faire

$$\frac{1+\mathfrak{M}N}{a}=\alpha,$$

ce qui donnerait $\alpha=a$, on pourrait faire

$$\frac{-1+\mathfrak{M}N}{a}=\alpha,$$

et de cette manière, α serait différent de a, et égal à $N-a$, comme cela est manifeste.

On peut donc toujours associer les nombres a, b, c, etc., deux à deux, de manière que leur produit soit ou $1+\mathfrak{M}N$ ou $-1+\mathfrak{M}N$; ainsi l'on peut dire que, quel que soit N, le produit de tous les nombres inférieurs et premiers à N est toujours de la forme $\pm 1+\mathfrak{M}N$, et que par conséquent l'un ou l'autre des facteurs

$$a.b.c.\ldots\overline{N-1}+1, \quad \text{ou} \quad a.b.c.\ldots\overline{N-1}-1,$$

est divisible par N comme nous l'avions avancé.

22. Il s'agit maintenant de reconnaître ces deux cas. Nous avons déjà remarqué que parmi les nombres a, b, c, d, etc., $N-1$, il y a toujours deux nombres x et $N-x$ qui sont tels qu'on a

$$\frac{1+\mathfrak{M}N}{x}=x \quad \text{ou} \quad 1+\mathfrak{M}N=x^2;$$

ce sont les deux nombres 1 et $N-1$; mais il peut y en avoir d'autres suivant la nature du nombre N.

Or, si N est tel qu'il y ait un nombre pair de ces couples qui puissent donner $1+\mathfrak{M}N=x^2$, il y aura un nombre pair d'expressions de la forme

$$-1+\mathfrak{M}N=x(N-x);$$

le produit total sera donc de la forme $1+\mathfrak{M}N$, et, dans ce cas, ce sera le facteur $a.b.c.d\ldots\overline{N-1}-1$ qui sera divisible par N.

Mais si le nombre de ces couples dont le produit est de la forme $-1+\mathfrak{M}N$, est impair, le produit total sera aussi de la forme $-1+\mathfrak{M}N$, et alors ce sera le facteur $a.b.c.d\ldots\overline{N-1}+1$ qui sera divisible par N.

23. Ainsi tout se réduit à reconnaître, d'après la nature du nombre N, si l'équation

$$x^2-1=\mathfrak{M}N$$

a des solutions conjuguées x et $N-x$, en nombre pair ou en nombre impair.

Or, je dis que l'équation

$$x^2-1=\mathfrak{M}N, \quad \text{ou} \quad (x+1)(x-1)=\mathfrak{M}N,$$

a autant de couples de ces solutions conjuguées, qu'il y a de manières de partager N en deux facteurs P et Q premiers entre eux, ou n'ayant tout au plus que le commun diviseur 2.

En effet, il est clair que les deux binômes $x+1$ et $x-1$, ou sont premiers entre eux, ou n'ont pas de plus grand commun diviseur que 2. Donc leur produit ne peut être divisible par N qu'autant qu'un de ces binômes $x+1$ le sera par un facteur P de N, et le second binôme $x-1$ par l'autre facteur Q (ces deux facteurs étant ou premiers

entre eux, ou sans autre commun diviseur que 2). Et réciproquement, on voit qu'à chacune de ces décompositions de N dans les deux facteurs P et Q, répondra un couple de valeurs de x, pour la résolution de l'équation

$$(x+1)(x-1) = \mathfrak{M}N.$$

Et si l'on veut trouver ces valeurs, on fera d'abord

$$x+1 = mP, \quad \text{et en même temps} \quad x-1 = m'Q,$$

ce qui donne

$$mP - m'Q = 2,$$

équation toujours possible puisque P et Q sont premiers entre eux, ou le deviennent en les divisant par le nombre 2 qui forme le second membre; on en tirera donc les valeurs des multiples m et m', et de là la valeur de x.

Ensuite, changeant l'ordre des facteurs P et Q, on ferait

$$x+1 = \mu Q, \quad \text{et} \quad x-1 = \mu' P,$$

et l'on trouverait de même

$$\mu Q - \mu' P = 2,$$

d'où l'on tirerait les nouveaux multiples μ et μ', et de là, la valeur conjuguée de x; mais ce calcul est inutile, puisque cette seconde valeur est évidemment $PQ - x$. En effet, si des deux binômes $x+1$, $x-1$, le premier est divisible par P et le second par Q, il s'ensuit qu'en changeant x en $PQ - x$, le premier, au contraire, devient divisible par Q et le second par P.

Ainsi donc on a pour l'équation

$$x^2 - 1 = \mathfrak{M}N, \quad \text{ou} \quad 1 + \mathfrak{M}N = x^2,$$

autant de couples de valeurs de x qu'il y a de manières de partager N en deux facteurs soit premiers entre eux, soit dépourvus de tout autre commun diviseur que 2.

24. Or, soit d'abord N *impair* ou *double* d'un impair; il n'y a lieu qu'à des décompositions de ce nombre en facteurs premiers entre eux : et si k marque le nombre des facteurs simples qui entrent dans N, on

sait que le nombre de ces décompositions est marqué par 2^{k-1}. (*Voyez* plus loin le nº **29.**) Ainsi ce nombre est toujours pair, excepté lorsqu'on a $k = 1$, ce qui répond au cas où le nombre N n'a qu'un seul facteur simple, c'est-à-dire est de la forme p^m, p étant un nombre premier.

Donc, pour $N = p^m$, c'est-à-dire *pour une puissance quelconque m d'un nombre premier p impair, on a toujours*

$$1.a.b.c.d \ldots \overline{N-1} + 1 = \mathfrak{M} N;$$

ce qui renferme, comme cas particulier, le théorème de Wilson, en faisant $m = 1$.

Si $N = 2p^m$, on a bien deux décompositions possibles de N en deux facteurs premiers entre eux, savoir, 1 et $2p^m$, et puis 2 et p^m; mais ces deux décompositions répondent aux mêmes solutions de

$$x^2 - 1 = \mathfrak{M}(2p^m),$$

puisque si l'un des binômes $x + 1$ et $x - 1$ est divisible par $2p^m$ et par conséquent par 2, l'autre est aussi divisible par 2. Ainsi, dans le cas de $N = 2p^m$, p étant un nombre premier quelconque, excepté 2, il n'y a encore qu'un seul couple de solutions possibles pour

$$x^2 - 1 = \mathfrak{M} N;$$

et partant, on a, comme ci-dessus,

$$1.a.b.c.d \ldots \overline{N-1} + 1 = \mathfrak{M} N;$$

mais pour tous les autres cas de N *impair* ou *simplement pair*, on a

$$1.a.b.c.d \ldots \overline{N-1} - 1 = \mathfrak{M} N.$$

25. Soit à présent N *pairement pair* ou d'un degré supérieur de parité; et soit k le nombre des facteurs simples qui entrent dans la composition de N; on aura d'abord 2^{k-1} pour le nombre de toutes les décompositions possibles en deux facteurs premiers entre eux, et puis encore 2^{k-1} pour le nombre des décompositions en deux facteurs non premiers entre eux, mais sans autre commun diviseur que 2; donc le nombre total des décompositions sera 2.2^{k-1} ou 2^k, et par conséquent

toujours pair, et l'on aura

$$1.a.b.c.d\,\text{etc.}\ \overline{N-1} - 1 = \mathfrak{M}N.$$

26. On exceptera pourtant le cas du nombre $N = 2.2$ ou 4; car à cause de la propriété de chacun des binômes $x+1$ et $x-1$, qui est de ne pouvoir être divisible par 2, sans que l'autre ne le soit en même temps, il est clair que les deux solutions de $x^2 - 1 = \mathfrak{M}4$ sont les mêmes, soit pour la décomposition de 4 en 1 et 4, soit pour la décomposition de 4 en 2 et 2, comme on l'a déjà remarqué plus haut, pour le cas de $N = 2p^m$.

27. Ainsi, pour nous résumer, *le produit de tous les nombres* 1, *a*, *b*, *c*, etc., N − 1, *inférieurs et premiers à* N, *étant augmenté de l'unité, est divisible par* N *dans tous les cas de* $N = p$ *ou* $2p$, *p étant un nombre premier quelconque; et dans le cas de* $N = p^m$ *ou* $2p^m$, *p étant un nombre premier quelconque, mais autre que le nombre* 2.

Pour tous les autres cas, le produit des nombres inférieurs et premiers à N, *étant, au contraire, diminué de l'unité, est toujours divisible par* N.

28. M. Gauss, dans ses *Disquisitiones arithmeticæ,* a indiqué cette extension du théorème de Wilson, pour des nombres quelconques N; mais comme il n'a point ajouté la démonstration des différents cas, il m'a paru assez intéressant d'éclaircir ce théorème qui dépend essentiellement de la résolution de l'équation binôme

$$x^2 - 1 = \mathfrak{M}N,$$

et du nombre des racines qu'elle admet suivant la nature du nombre donné N. On a vu d'ailleurs comment cette équation indéterminée se résout tout de suite au moyen d'une autre qui n'est que du premier degré, et dont la solution s'obtient par les méthodes connues.

Article V.

Sur toutes les décompositions possibles d'un nombre en deux facteurs premiers entre eux.

29. J'ai dit plus haut que le nombre de manières de décomposer $N = a^\alpha b^\beta c^\gamma \ldots$, en deux facteurs P et Q premiers entre eux, était marqué par 2^{k-1}, *k* étant le nombre des facteurs simples *a*, *b*, *c*,... qui

entrent dans la composition de N. On peut facilement démontrer ce théorème, comme le fait Legendre, en le tirant comme cas particulier d'un autre théorème où l'on considère tous les diviseurs possibles du nombre N; mais on peut aussi le démontrer directement et de la manière la plus simple, par la considération suivante. Et d'abord, puisque P et Q sont supposés premiers entre eux, on voit que chacun des diviseurs simples a, b, c,... ne peut jamais entrer que dans un seul des deux facteurs P et Q. Et par conséquent les exposants α, β, γ,... de ces diviseurs simples n'influent en aucune sorte sur le nombre cherché, qui est le même que si l'on avait simplement $N = abc...$ et qui ne dépend ainsi que du nombre k de ces diviseurs simples a, b, c, etc.; or, si l'on veut compter maintenant en combien de manières ce produit $abc...$ peut être partagé en deux facteurs P et Q, il n'y a qu'à voir de combien de manières on peut prendre les lettres a, b, c,... une à une, ce qui donne d'abord le nombre k; et puis ces mêmes lettres 2 à 2, ce qui donne $\frac{k.\overline{k-1}}{2}$; et puis ces mêmes lettres 3 à 3, ce qui donne $\frac{k.\overline{k-1}.\overline{k-2}}{2.3}$; et ainsi de suite jusqu'aux combinaisons $k-1$ à $k-1$; et l'on aura d'abord le nombre

$$k + \frac{k.\overline{k-1}}{2} + \frac{k.\overline{k-1}.\overline{k-2}}{2.3} + \text{etc.},$$

qui sera double du nombre des décompositions que l'on considère, puisque celles qui répondent aux combinaisons 1 à 1, 2 à 2, 3 à 3, etc., sont les mêmes qui répondent respectivement aux combinaisons $k-1$ à $k-1$, $k-2$ à $k-2$, $k-3$ à $k-3$, etc. Donc, si l'on ajoute au nombre précédent le nombre 2 ou $1+1$, pour compter aussi deux fois la dernière décomposition de N dans les facteurs premiers entre eux 1 et N, on aura

$$1 + k + \frac{k.\overline{k-1}}{2} + \frac{k.\overline{k-1}.\overline{k-2}}{2.3} + \text{etc.} + 1,$$

qui sera double de toutes les décompositions possibles que nous cherchons. Mais il est évident que cette suite n'est autre chose que $(1+1)^k$ ou 2^k; donc, en divisant par 2, on a pour le nombre cherché 2^{k-1}, comme nous l'avions supposé.

CHAPITRE II.

Démonstrations nouvelles des théorèmes qui précèdent.

Quoique les démonstrations que j'ai indiquées plus haut soient assez claires, il me semble qu'on en pourrait encore désirer de plus simples et de plus directes, surtout pour des théorèmes si élégants et si utiles dans la science des nombres.

Voici donc, en premier lieu, une nouvelle démonstration très-simple du fameux théorème de Fermat, que j'étendrai sur-le-champ à un nombre quelconque N simple ou composé.

ARTICLE Ier.

Théorème de Fermat généralisé.

1. Soient

$$1, a, b, c, d, \text{etc.}, N-1,$$

les n nombres inférieurs et premiers à un nombre quelconque N.

Multipliez tous ces nombres par l'un quelconque d'entre eux, x, autre que l'unité; ce qui donnera

$$x, \quad ax, \quad bx, \quad cx, \quad dx, \quad \text{etc.}, \quad \overline{N-1}.x,$$

il est clair que ces n produits seront tous différents entre eux, et de plus premiers à N; et que, par conséquent, étant rabaissés au-dessous de N par la division, ils ramèneront dans un autre ordre la première suite

$$1, a, b, c, d, \text{etc.}, N-1.$$

Donc le produit de ces nouveaux nombres x, ax, bx, etc., qui est $x^n(abc\ldots\overline{N-1})$, sera équivalent au produit des premiers $(abcd\ldots\overline{N-1})$, relativement au nombre N; de sorte qu'on aura

$$x^n(abcd\ldots N-1) = (abcd\ldots\overline{N-1}) + \mathfrak{M}N,$$

et, divisant de part et d'autre par $(abcd\ldots N-1)$, qui est un produit premier à N, il viendra

$$x^n = 1 + \mathfrak{M}N,$$

$\mathfrak{M}$ désignant un multiple nécessairement entier. C'est-à-dire que la puissance n d'un nombre quelconque x premier à N, étant diminuée de l'unité, est toujours divisible par N; de sorte qu'on a toujours

$$x^n - 1 = \mathfrak{M}N,$$

ce qu'il fallait démontrer.

Article II.

Théorème de Wilson généralisé, etc.

2. On peut démontrer d'une manière aussi simple le théorème général analogue au théorème de Wilson, que j'ai présenté plus haut, mais qui embrasse à la fois tous les nombres N simples ou composés.

Formez tous les produits $n - 1$ à $n - 1$, des n nombres 1, a, b, c, d, etc., $N - 1$, inférieurs et premiers à N; et vous aurez n produits différents entre eux, tous premiers à N, et qui, étant rabaissés au-dessous de N par la division, reviendraient aux n premiers nombres proposés 1, a, b, c, d, etc., $N - 1$, mais dans un nouvel ordre, ce qui est indifférent pour notre objet. Or il est évident que le produit de ces n produits différents est $(abcd\ldots\overline{N-1})^{n-1}$; et comme ce produit doit revenir au même, relativement à N, que le simple produit $(abcd\ldots\overline{N-1})$, il s'ensuit qu'on a

$$(abcd\ldots\overline{N-1})^{n-1} = (abcd\ldots\overline{N-1}) + \mathfrak{M}N,$$

ou bien

$$(abcd\ldots N - 1)^n = (abcd\ldots\overline{N-1})^2 + \mathfrak{M}N.$$

Mais par le théorème précédent, le premier membre $(abcd\ldots N - 1)^n$ est égal à l'unité; donc on a

$$(abcd\ldots\overline{N-1})^2 - 1 = \mathfrak{M}N;$$

c'est-à-dire que le *carré du produit de tous les nombres inférieurs et premiers à un nombre quelconque* N, *étant diminué de l'unité, est toujours divisible par* N.

3. En considérant les puissances quelconques

$$1,\ a^q,\ b^q,\ c^q,\ \text{etc.},\ \overline{N-1}^q,$$

on démontrerait de même que leur somme donnerait, relativement à N, le même reste que la somme des nombres

$$x^q,\ x^q a^q,\ x^q b^q,\ x^q c^q,\ \text{etc.},\ x^q\,\overline{N-1}^{\,q},$$

et que, par conséquent, la différence

$$(x^q - 1)\left(1 + a^q + b^q + \text{etc.} + \overline{N-1}^{\,q}\right)$$

est toujours divisible par N.

Si N est un nombre premier p, et q une puissance inférieure à $p-1$, le facteur binôme $x^q - 1$, qui ne peut devenir divisible par p pour plus de q valeurs de x, ne le sera donc point pour tous les nombres x, 1, 2, 3, 4, etc., jusqu'à $p-1$. Donc, en employant pour x une des valeurs qui ne donnent point $x^q - 1$ divisible par p, on en conclura que la somme des puissances q de tous les nombres

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ \text{etc.},\ p-1,$$

est toujours divisible par p, q étant inférieur à $p-1$; et même, comme on le verra plus loin, q étant un nombre quelconque, mais non divisible par $p-1$.

Remarque sur ces démonstrations et sur les deux principes qui leur servent de base.

4. Les démonstrations précédentes sont d'autant plus remarquables qu'elles ne supposent absolument que ces deux principes d'arithmétique : l'un, que *le résultat d'un produit est toujours le même dans quelque ordre que l'on multiplie les facteurs;* l'autre, que *si deux nombres sont premiers par rapport à un troisième, leur produit est aussi premier par rapport à ce troisième nombre.*

5. Le *premier principe,* qui permet de changer à volonté l'ordre de plusieurs facteurs a, b, c, d, e, h, sans troubler le résultat final de l'opération, est pour ainsi dire évident. Car on voit d'abord qu'on peut changer l'ordre de deux facteurs voisins.

Je suppose, en effet, que l'opération soit faite en suivant cet ordre

$$a.b.\bar{c}.\bar{d}.e.h,$$

et qu'on change l'ordre des deux facteurs voisins c et d, en sorte qu'on

ait actuellement

$$a.b.\dot{d}.\dot{c}.e.h,$$

je dis que les produits seront les mêmes. Car, supprimez le dernier facteur *h*, ce qui ne trouble pas l'égalité, si elle existe; supprimez ensuite, et par la même raison, le facteur *e*; il suffit de démontrer l'égalité des produits *abcd* et *abdc*; or, soit *p* le résultat commun *ab*, et il ne reste qu'à prouver l'égalité

$$p.c.d = p.d.c;$$

mais le premier produit peut se figurer ainsi :

$$d\left\{\begin{array}{l}\overbrace{p\ p\ p\ p\ p\ p\ p\ p,}^{c}\\ p\ p\ p\ p\ p\ p\ p\ p,\\ p\ p\ p\ p\ p\ p\ p\ p,\\ p\ p\ p\ p\ p\ p\ p\ p,\end{array}\right.$$

où l'on voit *p* pris *c* fois dans la ligne horizontale, et toute cette ligne $p \times c$ prise *d* fois.

Mais on y voit également *p* pris *d* fois dans la ligne verticale, et toute cette ligne $p \times d$ prise *c* fois.

Ainsi, le produit $p \times c \times d$, non-seulement est égal au produit $p \times d \times c$, mais il est encore *identique* avec lui : c'est la même chose vue de deux manières différentes.

Actuellement il est clair que le produit de tant de facteurs qu'on voudra est identique avec le produit des mêmes facteurs pris dans un nouvel ordre quelconque. Car, par le théorème précédent, vous pouvez amener un facteur quelconque à la place de son voisin, et par conséquent, de proche en proche, à telle place que vous voudrez. Vous pourrez donc, sans changer l'un des deux produits, mettre ses différents facteurs précisément dans l'ordre où ils sont écrits dans l'autre, auquel cas l'identité de ces deux produits est manifeste.

6. Le *second principe* se trouve démontré dans les *Éléments d'Euclide;* j'en ai donné, il y a longtemps, une démonstration facile, qui

a déjà passé dans quelques ouvrages, et que je crois devoir rapporter ici, à cause de sa simplicité.

Si deux nombres a et b sont premiers à N, *leur produit sera aussi premier à* N.

En effet, faites la même opération que si vous cherchiez le plus grand commun diviseur entre a et N; comme, par hypothèse, ils n'en ont pas d'autre que l'unité, vous trouverez une suite d'équations telles que celles-ci :

$$\begin{aligned} a &= \mathrm{N}.q + \mathrm{R}, \\ \mathrm{N} &= \mathrm{R}.q' + \mathrm{R}', \\ &\ldots\ldots \\ \mathrm{R} &= \mathrm{R}'.q'' + 1, \end{aligned}$$

où la dernière présentera nécessairement pour dernier reste l'unité.

Multipliez toutes ces équations par b, et vous aurez

$$\begin{aligned} ab &= b\mathrm{N}\,q + b\mathrm{R}, \\ b\mathrm{N} &= b\mathrm{R}\,q' + b\mathrm{R}', \\ &\ldots\ldots \\ b\mathrm{R} &= b\mathrm{R}'q'' + b. \end{aligned}$$

Or, s'il existait un commun diviseur θ entre ab et N, vous voyez, par la première équation, qu'il diviserait nécessairement bR; et par la deuxième équation, qu'il diviserait nécessairement bR', etc.; et par la dernière enfin, qu'il diviserait nécessairement b: ainsi, θ diviserait nécessairement N et b, ce qui ne se peut, puisque b est premier à N. Donc ab est premier à N.

Mais on peut encore tirer ce théorème de principes plus simples puisés dans la considération de l'*ordre*, comme nous le verrons dans le chapitre suivant.

Article III.

Sur le nombre qui marque combien il y a de nombres inférieurs et premiers à un nombre donné.

7. Quant au nombre n qui marque combien il y a de nombres inférieurs et premiers à un nombre donné N, on sait qu'il dépend de N et des facteurs simples qui entrent dans sa composition : de sorte que si



ces facteurs simples sont représentés par α, β, γ, etc., on a toujours

$$n = N\left(1 - \frac{1}{\alpha}\right)\left(1 - \frac{1}{\beta}\right)\left(1 - \frac{1}{\gamma}\right) \text{ etc.}$$

Euler a démontré le premier ce théorème en plusieurs endroits des *Mémoires de Saint-Pétersbourg*. M. Legendre et M. Gauss en ont aussi donné la démonstration dans leurs ouvrages; mais il me semble qu'on en peut encore présenter une autre plus simple, et qui s'offre, pour ainsi dire, d'elle-même dans la question proposée.

En effet, si de la suite des nombres 1, 2, 3, 4,... jusqu'à N, on ôte tous les multiples de α; que des nombres restants on ôte tous les multiples de β, et ainsi de suite; il est clair qu'on aura ôté tous les nombres qui peuvent avoir avec N quelque commun diviseur. Ainsi les nombres restants, qui ne peuvent contenir aucun des facteurs simples de N, seront nécessairement premiers à N. Il s'agit donc d'examiner combien il doit rester successivement de ces nombres, à mesure qu'on retrancherait de la suite

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ldots,\ N$$

tous les multiples de α; et du reste tous les multiples de β; et du nouveau reste les multiples de γ, et ainsi de suite.

Or, il est évident que le nombre des multiples de α, contenus dans la suite précédente, est le sous-multiple α du nombre N de tous les termes, c'est-à-dire est $\frac{N}{\alpha}$: car on ne trouve ces multiples de α, qu'en prenant les termes de α en α, à partir du premier 1; on aura donc, pour le nombre N' des termes restants, quand on ôte les $\frac{N}{\alpha}$ multiples de α,

$$N' = N - \frac{N}{\alpha},$$

ou bien

$$N' = N\left(1 - \frac{1}{\alpha}\right).$$

Actuellement, de ces N' nombres il faut ôter les multiples de β; or je dis qu'il y en a la même partie aliquote que dans les N premiers, c'est-à-dire qu'il y en a $\frac{N'}{\beta}$. En effet, je puis voir ces N' termes comme com-

posés de la suite des N premiers, moins la suite des multiples de α qu'on a soustraits; or, dans la première suite, il y a $\frac{N}{\beta}$ multiples de β, et dans la seconde, qui est aussi une progression arithmétique, il est clair qu'il y en a la même aliquote. Donc, dans les N' termes qui font comme la différence des deux suites, il y en a aussi la même aliquote, c'est-à-dire $\frac{N'}{\beta}$. Donc on a, comme plus haut, en marquant par N'' le nombre des termes qui restent,

$$N'' = N'\left(1 - \frac{1}{\beta}\right).$$

Maintenant, de ces nombres restants il faut ôter tous les multiples de γ: or je dis que dans ces N'' termes restants, il y en a encore la même aliquote que dans les N premiers et dans les N' seconds; c'est-à-dire qu'il y en a $\frac{N''}{\gamma}$. Car je puis voir ces N'' termes restants comme composés des N' précédents, moins les $\frac{N'}{\beta}$ multiples de β qui y sont contenus.

Or, dans la première suite des N' termes, il est clair, comme ci-dessus, qu'il y a $\frac{N'}{\gamma}$ multiples de γ; et dans la seconde, qui est composée des $\frac{N'}{\beta}$ multiples de β, il est facile de voir qu'il y en a aussi la même aliquote (car cette suite n'est autre chose que les multiples de β pris dans N, moins les multiples de β pris dans les $\frac{N}{\alpha}$ multiples de α); donc, dans la différence N'', il y a $\frac{N''}{\gamma}$ multiples de γ; donc, en ôtant les multiples de γ, on aura pour le nombre N''' de ceux qui restent :

$$N''' = N''\left(1 - \frac{1}{\gamma}\right),$$

et ainsi de suite.

Ainsi l'on a

$$N' = N\left(1 - \frac{1}{\alpha}\right),$$
$$N'' = N\left(1 - \frac{1}{\alpha}\right)\left(1 - \frac{1}{\beta}\right),$$
$$N''' = N\left(1 - \frac{1}{\alpha}\right)\left(1 - \frac{1}{\beta}\right)\left(1 - \frac{1}{\gamma}\right), \text{ etc.},$$

et par conséquent

$$n = N\left(1 - \frac{1}{\alpha}\right)\left(1 - \frac{1}{\beta}\right)\left(1 - \frac{1}{\gamma}\right)\cdots,$$

ce qu'il fallait démontrer.

Remarque I.

8. Cette démonstration très-simple résulte, comme on voit, de ce principe que, dans les diverses suites de nombres que l'on considère, il y a toujours la même aliquote des multiples d'un même facteur. Ainsi, quand des N premiers nombres ou multiples de 1, on veut ôter les multiples de α et compter ceux qui restent, il faut retrancher une partie $\frac{1}{\alpha}$ de ces N nombres, ou multiplier N par $1 - \frac{1}{\alpha}$: et parmi ces nombres restants, il y a encore proportionnellement autant de multiples de β, qu'il y en a dans les N premiers, et par conséquent il y en a une partie $\frac{1}{\beta}$. Donc, si l'on veut les ôter et compter ceux qui restent, il faut multiplier le premier résultat $N\left(1 - \frac{1}{\alpha}\right)$ par $1 - \frac{1}{\beta}$, et ainsi de suite.

Dans les *Mémoires de Saint-Pétersbourg* pour 1780, je trouve qu'Euler a présenté une démonstration semblable qu'il regarde, avec raison, comme la plus simple, et dont l'idée lui avait été donnée par la manière même dont se compose la formule précédente, qu'il avait déjà trouvée par une autre analyse. Mais il y a une remarque importante à faire sur cette dernière démonstration : c'est qu'Euler y suppose précisément ce qui en fait toute la force, je veux dire, qu'il y a toujours la même aliquote des multiples d'un même facteur dans ces diverses suites où le nombre des termes est N, N', N'', etc. Or cela ne se voit clairement que pour la première suite, car les autres cessent d'être des progressions par différence, et deviennent de plus en plus irrégulières. Ainsi l'auteur omet le seul point essentiel de la démonstration, le reste n'ayant aucune difficulté, et le théorème ne se trouvait point par là solidement établi.

Remarque II.

9. Le nombre N étant par hypothèse de la forme $N = \alpha^{\lambda}\beta^{\mu}\gamma^{\nu}\ldots$,

l'expression précédente de n, qui est

$$n = \mathrm{N}\left(1 - \frac{1}{\alpha}\right)\left(1 - \frac{1}{6}\right)\left(1 - \frac{1}{\gamma}\right)\ldots,$$

peut se réduire à celle-ci

$$n = \alpha^{\lambda-1}(\alpha - 1).6^{\mu-1}(6 - 1).\gamma^{\nu-1}(\gamma - 1)\ldots,$$

où l'on voit facilement que, *si le nombre* $\mathrm{N} = \alpha^{\lambda} 6^{\mu} \gamma^{\nu}\ldots$ *est partagé en facteurs quelconques* P, Q, R,... *premiers entre eux, le nombre* n, *qui marque combien il y a de nombres inférieurs et premiers à* N, *est égal au produit de ceux qui marqueraient de même combien il y a de nombres inférieurs et premiers à chacun des facteurs* P, Q, R,... *de* N.

Ainsi en indiquant, comme le fait Euler, par le signe $\varphi(\mathrm{N})$ la multitude des nombres inférieurs et premiers à un nombre N, si l'on suppose ce nombre décomposé d'une manière quelconque en facteurs P, Q, R, etc., premiers entre eux, on a ce théorème élégant

$$\varphi(\mathrm{N}) = \varphi(\mathrm{PQR}\ldots) = \varphi(\mathrm{P}).\varphi(\mathrm{Q}).\varphi(\mathrm{R})\ldots.$$

Remarque III.

10. Si l'on décomposait N dans les deux facteurs 1 et N qui sont premiers entre eux, on aurait donc

$$\varphi(\mathrm{N}) = \varphi(1)\,\varphi(\mathrm{N}),$$

d'où l'on voit qu'il faut compter $\varphi(1)$ comme égal à 1. Cependant on ne peut pas dire qu'il y ait aucun nombre *inférieur* et premier à 1; mais on peut dire qu'il y a un nombre premier à 1 et *non plus grand* que 1, et qui est 1 lui-même; car ces deux nombres 1 et 1, quoiqu'ils soient égaux, doivent être regardés, suivant la définition, comme premiers entre eux, puisqu'ils n'ont d'autre commun diviseur que l'unité. C'est, au reste, une propriété qui n'appartient qu'à ces seuls nombres égaux. Donc, si l'on veut envelopper aussi ce cas unique dans la même expression commode que j'ai employée jusqu'ici, il faut entendre, par nombre premier et *inférieur* à un autre, un nombre premier à cet autre et *non plus grand*. Et de cette manière, ce cas singulier qui regarde l'unité se trouvera compris parmi tous les autres.

Remarque IV.

11. L'expression générale du nombre n fait voir encore que n est toujours pair, excepté dans le cas de

$$N = 1 \quad \text{et} \quad N = 2,$$

où l'on a

$$\varphi(1) = 1 \quad \text{et} \quad \varphi(2) = 1.$$

Si $N = 2I$, I étant un nombre impair, on a

$$\varphi(N) = \varphi(I)\,\varphi(2),$$

et partant

$$\varphi(2I) = \varphi(I).$$

Ainsi il n'y a pas plus de nombres inférieurs et premiers au double d'un impair, qu'à cet impair lui-même. En géométrie, j'ai fait voir qu'il y a autant d'espèces de polygones réguliers de N côtés, qu'il y a de nombres inférieurs et premiers à N, ou simplement la moitié, si l'on ne veut compter que les polygones qui font à nos yeux des images différentes. On voit donc que, pour les polygones de $2I$ côtés, il n'y a pas plus d'espèces différentes que pour les polygones d'un nombre I de côtés, deux fois moindre. Ainsi, il n'y a pas plus d'espèces d'hexagones que d'espèces de triangles; pas plus de décagones que de pentagones, etc., mais ce sont les seuls cas où la chose ait lieu; car 2 est, après l'unité, le seul nombre qui donne $\varphi(2) = 1$.

ARTICLE IV.

Sur le nombre de tous les diviseurs possibles d'un nombre donné.

12. Considérons maintenant tous les diviseurs possibles que peut avoir un nombre $N = \alpha^\lambda \beta^\mu \gamma^\nu \ldots$, en y comprenant 1 et le nombre N lui-même. Il est clair que ces diviseurs ne sont autre chose que les différents termes du produit fait de ces progressions géométriques

$$\begin{array}{l}
1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 + \ldots + \alpha^\lambda, \\
1 + \beta + \beta^2 + \beta^3 + \beta^4 + \ldots + \beta^\mu, \\
1 + \gamma + \gamma^2 + \gamma^3 + \gamma^4 + \ldots + \gamma^\nu, \\
\ldots\ldots\ldots\ldots\ldots\ldots
\end{array}$$

D'où l'on voit, par la théorie des combinaisons, que le *nombre total* de ces termes est exprimé par

$$(\lambda + 1)(\mu + 1)(\nu + 1)\ldots.$$

Quant à la *somme* de ces mêmes termes, elle est le produit de nos progressions géométriques, et par conséquent

$$\frac{\alpha^{\lambda+1}-1}{\alpha-1}\cdot\frac{6^{\mu+1}-1}{6-1}\cdot\frac{\gamma^{\nu+1}-1}{\gamma-1}\ldots.$$

Sur le nombre qui marque combien il y a de nombres inférieurs et premiers à tous les diviseurs possibles d'un nombre donné.

13. Mais supposons ici qu'on veuille compter combien il y a de nombres inférieurs et premiers à tous ces diviseurs possibles. Si l'on ne regarde d'abord que les diviseurs élémentaires qui forment les termes de nos progressions, on aura ces différentes suites:

$$1 + \varphi(\alpha) + \varphi(\alpha^2) + \varphi(\alpha^3) + \ldots + \varphi(\alpha^\lambda),$$
$$1 + \varphi(6) + \varphi(6^2) + \varphi(6^3) + \ldots + \varphi(6^\mu),$$
$$1 + \varphi(\gamma) + \varphi(\gamma^2) + \varphi(\gamma^3) + \ldots + \varphi(\gamma^\nu),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Or, en vertu du théorème précédent (n° 9), il est manifeste que si l'on fait le produit de ces séries, on aura pour résultat une suite de termes dont chacun marquera combien il y a de nombres inférieurs et premiers à chaque terme du produit de nos progressions, et par conséquent, à tous les diviseurs possibles de N; mais chaque série

$$1 + \varphi(\alpha) + \varphi(\alpha^2) + \varphi(\alpha^3) + \ldots + \varphi(\alpha^\lambda)$$

vaut $\quad 1 + (\alpha - 1) + \alpha(\alpha - 1) + \alpha^2(\alpha - 1) + \ldots + \alpha^{\lambda-1}(\alpha - 1),$

c'est-à-dire vaut 1 plus une progression géométrique dont la somme est $\alpha^\lambda - 1$; donc la première série vaut en somme $1 + \alpha^\lambda - 1$, c'est-à-dire α^λ. De même la deuxième série vaut en somme 6^μ, et la troisième γ^ν, et ainsi des autres; donc le produit de ces suites, ou le nombre cherché, est $\alpha^\lambda 6^\mu \gamma^\nu\ldots$, c'est-à-dire le nombre N lui-même.

On a donc ce théorème remarquable et qui nous sera utile dans la théorie des *racines primitives :*

Si l'on considère tous les diviseurs possibles d'un nombre quelcon-

que N, et qu'on veuille compter combien il y a de nombres inférieurs et premiers à chacun d'eux, on trouvera en somme totale le nombre N lui-même.

M. Gauss est, je crois, le premier qui ait donné ce théorème dans ses *Disquisitiones arithmeticæ;* mais sa démonstration, qui nous a paru un peu difficile, diffère en entier de la précédente. Il me semble que la nôtre est aussi directe et aussi claire qu'on puisse le désirer.

14. Avant de quitter ce sujet, j'ajouterai encore une proposition tres-simple qui peut aussi servir dans la théorie des nombres.

On a fait voir plus haut que, si un nombre quelconque N est résolu en différents facteurs premiers entre eux, P, Q, R, etc., le nombre n, qui marque combien il y a de nombres inférieurs et premiers à N, s'exprime facilement au moyen de ceux qui marquent combien il y a de nombres inférieurs et premiers aux différents facteurs P, Q, R,...: de sorte qu'on a cette formule élégante

$$n = \varphi(\mathrm{N}) = \varphi(\mathrm{PQR}...) = \varphi(\mathrm{P}).\varphi(\mathrm{Q}).\varphi(\mathrm{R})....$$

Or je vais démontrer que ces nombres premiers à N peuvent aussi s'exprimer à l'aide de ceux qui sont premiers aux facteurs P, Q, R,... de ce nombre composé N.

15. Soient e un nombre quelconque premier à N; et p, q, r,... des nombres respectivement premiers à ses facteurs P, Q, R,...; je dis qu'on aura, pour l'expression des nombres e premiers à N,

$$e = p\mathrm{QR} + q\mathrm{PR} + r\mathrm{PQ} + ...$$

En effet, il est aisé de voir que le second membre sera toujours premier à N. Car soit, s'il est possible, θ un nombre qui divise à la fois la somme

$$p\mathrm{QR} + q\mathrm{PR} + r\mathrm{PQ} + ...$$

et le nombre

$$\mathrm{N} = \mathrm{PQR}...;$$

θ diviserait nécessairement un des facteurs P, Q, R,... puisque ces facteurs sont premiers entre eux par l'hypothèse. Or, dans l'expression de e, qui est

$$p\mathrm{QR} + q\mathrm{PR} + r\mathrm{PQ} + ...,$$

ce facteur P, que θ diviserait, entre dans tous les termes, hors dans un seul ; tous ces termes sont donc divisibles par θ; la somme entière doit l'être aussi par hypothèse; donc le seul terme pQR où P n'entre pas doit l'être aussi : mais ni Q, ni R, etc., ne peuvent l'être par θ puisqu'ils sont premiers à P; donc p devrait être divisible par θ, aussi bien que P; donc p ne serait pas premier à P, contre l'hypothèse. Donc

$$e = p\mathrm{QR} + q\mathrm{PR} + r\mathrm{PQ} + \ldots$$

est premier à PQR..., *ce qu'il fallait démontrer.*

16. En prenant pour $p, q, r, \ldots$ tous les nombres respectivement inférieurs à P, Q, R,..., on aura, par la théorie des combinaisons,

$$\varphi(\mathrm{P}).\varphi(\mathrm{Q}).\varphi(\mathrm{R})\ldots$$

pour le nombre des valeurs de e; et il est aisé de voir que toutes ces valeurs seront différentes entre elles relativement au module N.

En effet, soient, s'il est possible, deux valeurs

$$p\,\mathrm{QR} + q\,\mathrm{PR} + r\,\mathrm{PQ} + \ldots,$$
$$p'\mathrm{QR} + q'\mathrm{PR} + r'\mathrm{PQ} + \ldots,$$

qui donneraient le même nombre e premier à N; il faudrait que la différence

$$(p-p')\,\mathrm{QR} + (q-q')\,\mathrm{PR} + (r-r')\,\mathrm{PQ} + \ldots,$$

fût divisible par

$$\mathrm{N} = \mathrm{PQR}\ldots$$

et je dis que cela est impossible, à moins qu'on n'ait

$$p = p', \quad q = q', \quad r = r', \quad \text{etc.}$$

Car si cette différence est divisible par PQR..., à plus forte raison le sera-t-elle par le facteur P; mais tous les termes le sont par P, hors le premier $(p-p')$QR; donc il faudrait que celui-ci le fût; mais Q, R,... sont premiers à P; donc il faudrait que $p - p'$ fût divisible par P, ce qui ne se peut, puisque p et p' sont deux nombres différents inférieurs à P.

Ainsi les deux expressions précédentes ne peuvent donner le même nombre e, à moins qu'on n'ait $p' = p$; et, par une raison toute semblable, $q' = q$, $r' = r$, etc., auquel cas ces expressions se confondent.

Donc la formule

$$e = pQR + qPR + rPQ + \ldots,$$

en y prenant pour p un nombre inférieur et premier à P, pour q un nombre inférieur et premier à Q, etc., est l'expression générale des nombres e premiers à $N = PQR\ldots$, et elle n'en donne qu'un nombre $\varphi(P).\varphi(Q).\varphi(R)\ldots$ de *différents*, comme cela doit être.

CHAPITRE III.

Démonstrations nouvelles tirées de la considération de l'ordre.

Il semble que les démonstrations précédentes sur les premières propriétés des nombres soient aussi simples qu'on puisse le désirer. Elles rattachent les théorèmes à quelques principes élémentaires, et elles en font voir en quelque sorte la liaison et la dépendance mutuelle. Cependant il faut convenir que l'esprit n'est pas encore conduit dans cette matière par une analyse bien directe, et qu'on ne voit pas ce qui a pu donner l'idée de ces théorèmes qui paraissent si curieux et si importants dans la théorie des nombres. Sans doute la considération des restes que donne la division des puissances successives d'un nombre par un même diviseur premier se présente assez naturellement en arithmétique, et c'est par là que les géomètres paraissent avoir commencé cette première partie de la théorie des nombres. Mais il me semble que ces théorèmes ont une source plus profonde dans la science des mathématiques, et qu'ils doivent tenir à des principes d'un ordre plus élevé, de manière à ce qu'on voie que ce n'est point par hasard que l'esprit s'est attaché à ces spéculations, qu'elles ne sont point de pure curiosité, mais puisées dans la nature même des choses, et qu'elles forment une partie fondamentale de la science mathématique considérée de la manière la plus générale : et, pour en donner une idée, je vais présenter de nouvelles démonstrations, uniquement tirées de la considération de l'*ordre* qu'on peut observer actuellement entre plusieurs objets.

1. Considérons donc plusieurs objets a, b, c, d, e, etc., situés d'une manière quelconque dans l'espace, et regardons-les d'abord dans un

certain ordre tel que celui-ci : a, b, c, d, e, etc., de manière qu'après a vienne b, ensuite c, ensuite d, etc. : et comme ici nous n'avons en vue que le nombre et l'ordre, supposons que tous ces objets soient égaux, à égales distances l'un de l'autre, et simplement représentés par N points a, b, c, d, etc., rangés en cercle, et formant ainsi les sommets d'un polygone régulier de N côtés.

Cela posé, si à partir de l'un d'eux, comme du point a par exemple, on va de l'un à l'autre en les prenant successivement de 2 en 2, ou de 3 en 3, ou en général de h en h, et que cet intervalle constant h par lequel on saute soit premier à N, je dis qu'on passera nécessairement par tous les points a, b, c, d, etc., avant de revenir au point a d'où l'on est parti.

En effet, supposons qu'on ne passe que par une partie de ces N points ou sommets, c'est-à-dire par un nombre n d'entre eux, n étant inférieur à N ; on aurait donc formé un polygone régulier de n côtés, et dont chaque côté répondrait à un nombre h de côtés consécutifs sur le premier polygone. En suivant le contour entier de ce polygone, ce qui vous fera faire une ou plusieurs fois le tour du cercle, vous pourriez donc compter un nombre nh de points sur la route parcourue ; et comme vous êtes revenu au point de départ, par hypothèse, vous auriez ainsi ce nombre nh égal à un multiple exact des N points de la circonférence entière. Ainsi il faudrait que nh fût un multiple de N ; mais h est premier à N et n est inférieur à N ; donc le produit nh n'est pas divisible par N, et par conséquent n'en peut être un multiple.

Donc, pour que le produit nh soit un multiple exact de N, tel que qN, il faut nécessairement que n soit égal à N, et alors il s'ensuit que q est égal à h. D'où l'on conclut ce théorème :

Si l'on a N *points rangés en cercle, et qu'on les joigne de h en h, h étant premier à* N, *on passe nécessairement par tous les* N *points avant de retomber sur le point de départ ; et l'on fait nécessairement h fois le tour entier de la circonférence.*

2. Réciproquement, *si en joignant* N *points de h en h, on passe par tous ces points avant de revenir au premier, h sera nécessairement premier à* N. Car alors h ne pourra mesurer exactement de multiple de N, qui soit moindre que $h \times$ N ; et par conséquent la plus grande

aliquote de h qui puisse mesurer N, sera l'aliquote $\frac{h}{h}$ ou l'unité; et par conséquent h et N seront premiers entre eux.

Si donc en joignant ainsi plusieurs points par des intervalles quelconques égaux, on ne peut jamais revenir au premier sans avoir passé par tous les autres, on peut assurer que tous ces points sont en nombre premier absolument : ce qui donne une espèce de définition géométrique d'un nombre *premier*.

3. Si h *et* N *ne sont pas premiers entre eux, je dis qu'en joignant les* N *points de* h *en* h, *on ne passera que par* $\frac{N}{\theta}$ *d'entre eux;* θ *étant le plus grand commun diviseur des deux nombres* h *et* N.

Il est bien aisé de déduire cette proposition de la première, où h et N sont premiers entre eux; mais on peut aussi la démontrer directement de la manière suivante, et comprendre ainsi en un seul les deux théorèmes dont il s'agit.

Démonstration. Portez h sur la circonférence N jusqu'à ce que vous reveniez au point de départ (ce qui ne peut jamais manquer d'arriver après avoir fait h fois le tour du cercle au plus); vous aurez donc fait un certain nombre de fois q, le tour de la circonférence, et vous aurez le plus petit multiple qN que vous puissiez mesurer par le nombre h; donc la plus grande aliquote de h qui pourra mesurer N sera $\frac{h}{q}$, et par conséquent $\frac{h}{q}$ sera égal au plus grand commun diviseur de h et de N; de sorte qu'on aura

$$\frac{h}{q} = \theta, \quad \text{ou} \quad q = \frac{h}{\theta}.$$

Or, si l'on désigne par x le nombre des côtés h du polygone qu'on aura formé, lequel nombre x marquera aussi celui des sommets ou points par lesquels on aura passé, on aura évidemment le produit xh égal au multiple qN de la circonférence N : ce qui donne, à cause de q égal à $\frac{h}{\theta}$,

$$xh = \frac{Nh}{\theta}, \quad \text{et par conséquent,} \quad x = \frac{N}{\theta}.$$

Ainsi l'on ne passera que par un nombre x de points marqué par $\frac{N}{\theta}$; et l'on aura fait le tour entier de la circonférence un nombre de fois q, marqué par $\frac{h}{\theta}$; *ce qu'il fallait démontrer.*

4. Cette démonstration est générale pour deux nombres quelconques h et N. Si leur plus grand commun diviseur θ est égal à l'unité, les deux nombres sont premiers entre eux, et alors, à cause de $\theta = 1$, on a $x = N$, et $q = h$; ce qui redonne, comme conséquence, le premier théorème qu'on avait démontré.

5. On peut remarquer encore que cette démonstration ne suppose aucune propriété des nombres ni aucun théorème d'arithmétique, pas même cette théorie du plus grand commun diviseur que nous devons à Euclide. Elle donnerait même, au besoin, pour la recherche de ce commun diviseur, une règle nouvelle qu'on pourrait suivre en arithmétique et en géométrie, et qui ne paraît pas moins élégante.

Règle nouvelle pour trouver la plus grande commune mesure de deux grandeurs, ou le plus grand commun diviseur de deux nombres donnés.

6. Soit à trouver la plus grande commune mesure de deux grandeurs A et B; portez l'une d'elles A sur l'autre B, et si elle y est contenue exactement un certain nombre de fois, la grandeur A sera elle-même la commune mesure. Mais s'il y a un reste, au lieu de prendre ce reste et de le porter sur la première A, comme on le fait ordinairement, portez toujours la même grandeur A, non plus sur la grandeur simple B, mais sur le *double* de B; s'il n'y a pas de reste, la *moitié* de la première A mesure la seconde B, et c'est la plus grande commune mesure. S'il y a encore un reste, continuez toujours de porter A, mais sur le triple 3B de la seconde B; si elle y tombe un nombre exact de fois, le *tiers* de A sera la commune mesure de A et B, et ainsi de suite : de sorte que si la première grandeur A ne commence à mesurer juste que le multiple mB de la seconde, $\frac{A}{m}$ sera nécessairement la plus grande commune mesure des deux grandeurs A et B.

Et, en effet, s'il y avait une autre aliquote de A qui pût mesurer B,

telle que l'aliquote $\frac{A}{m'}$, et qui fût plus grande que $\frac{A}{m}$, ce qui donnerait $m' < m$; alors, comme $\frac{A}{m'}$ mesurerait B, il est évident que A mesurerait exactement m'B, et par conséquent un multiple de B, plus petit que le multiple mB : or cela ne se peut, puisque mB est le premier, et par conséquent le *plus petit* multiple de B que vous ayez pu mesurer par la grandeur A. Donc $\frac{A}{m}$ est la plus grande commune mesure 6 des deux grandeurs A et B.

Si, au lieu de prendre la grandeur A pour la porter sur B, on prend B pour la porter sur A, ou 2A, ou 3A, ou etc., jusqu'à ce qu'on rencontre le plus petit multiple nA que B mesure exactement, on aura de même $\frac{B}{n}$ pour la plus grande commune mesure des deux grandeurs proposées.

D'où l'on voit, en comparant cette seconde expression à la première, que le rapport $\frac{A}{B}$ sera exprimé par la fraction $\frac{m}{n}$, fraction qui se trouvera toute réduite à sa plus simple expression.

7. En *opérant sur les nombres,* on diviserait le nombre B par A, on aurait un certain quotient et un reste; on ajouterait à ce reste le dividende B, et l'on continuerait de diviser par A, et ainsi de suite jusqu'à ce qu'on parvînt à une division sans reste; alors on diviserait A par le nombre m de divisions effectuées, et $\frac{A}{m}$ serait la plus grande partie de A capable de mesurer B, ou le plus grand commun diviseur des deux nombres A et B. Mais le procédé serait plus long que par la méthode ordinaire.

8. En *Géométrie,* on prendrait une ligne indéfinie sur laquelle on porterait successivement des parties égales à l'une B des deux lignes données; on porterait ensuite l'autre ligne A, à partir d'un point de division, jusqu'à ce qu'on retombât sur un autre point de division, et si cela arrivait après avoir mesuré la longueur mB. $\frac{A}{m}$ serait la commune mesure.

9. Mais comme il faut toujours ajouter la ligne B à elle-même, ou prendre sur une ligne indéfinie tous les multiples de B, il est bien plus clair et plus simple de représenter la ligne B par une ligne fermée rentrante sur elle-même, telle, par exemple, que la circonférence d'un cercle; ou, si B marque un nombre, de le représenter par B points rangés régulièrement sur cette circonférence; alors on trouve sur la même figure finie, l'infinité des multiples de cette ligne, ou de ce nombre, en faisant toujours le tour du même cercle. Ainsi l'on portera la longueur ou le nombre A sur la circonférence B, à partir d'un point quelconque, jusqu'à ce qu'on revienne au point de départ; alors on aura fait un certain nombre m de fois le tour de la circonférence, et l'on aura le plus petit multiple mB qu'on puisse mesurer par la grandeur A; et par conséquent, on aura $\frac{A}{m}$ pour la plus grande commune mesure de A et B.

De cette manière, l'opération est plus simple que l'opération ordinaire; car, suivant le procédé connu, il faut porter A sur B, et puis le reste r sur A, et puis le nouveau reste r' sur le précédent r, et puis r'' sur r', et ainsi de suite; mais ici vous portez toujours la même grandeur A sur la même grandeur B, rentrante en elle-même, jusqu'à ce que vous retombiez au point de départ, ce qui ne fait qu'une seule et même opération. Il ne s'agit donc que de compter combien de fois vous avez fait le tour de B, et, si ce nombre est m, la $m^{ième}$ partie de A est la plus grande commune mesure. Si l'opération n'a pas de fin, les deux grandeurs sont *incommensurables*.

Mais je passe à d'autres propriétés des nombres, toujours déduites de la simple considération de l'ordre.

10. Et d'abord, ce théorème d'Euclide, rappelé au nº 6 du chapitre précédent, peut se voir de la manière la plus évidente.

Car soient toujours nos N points rangés en cercle dans l'ordre a, b, c, d, e, etc.; si, à partir de l'un d'eux, vous prenez ces points en les joignant de α en α, α étant un nombre inférieur et premier à N, vous passerez, comme on l'a dit, par tous les autres, et vous formerez ainsi un nouveau polygone régulier de N côtés. Actuellement, si dans ce nouveau polygone vous prenez les points de β en β, β étant aussi pre-

mier à N, vous aurez un troisième polygone de N côtés. Or il est évident que prendre d'abord les sommets de α en α, et ensuite, dans le polygone qui en résulte, les prendre de β en β, revient au même que de prendre tout d'un coup les sommets de $\alpha\beta$ en $\alpha\beta$ dans le premier polygone qu'on a considéré. Donc, puisqu'en prenant de $\alpha\beta$ en $\alpha\beta$, on passe par tous les N points, il s'ensuit, n° 2, que le produit $\alpha\beta$ est un nombre premier à N. On a donc ce principe fondamental dans la théorie des nombres : *Si deux nombres α et β sont premiers à un troisième nombre* N, *leur produit $\alpha\beta$ est aussi premier à ce troisième.* D'où l'on peut tirer cette suite de conséquences :

Que tant de nombres qu'on voudra, premiers à un autre nombre N, donnent leur produit aussi premier par rapport à ce nombre N;

Que α étant premier à N, toutes les puissances α^2, α^3, α^4, etc., sont aussi premières à N;

Qu'un nombre quelconque N ne peut se résoudre que d'une seule manière en facteurs premiers;

Que les racines des puissances imparfaites ne peuvent être exprimées par des fractions, et que, par conséquent, elles sont incommensurables avec l'unité; etc., etc.

11. Le théorème général d'Euler, exprimé par l'équation

$$x^n - 1 = \mathfrak{M}N,$$

où n marque combien il y a de nombres inférieurs et premiers à N, et $\mathfrak{M}$N un multiple quelconque de N, peut aussi se démontrer d'une manière simple et lumineuse par cette même considération de l'ordre.

Car soient N points a, b, c, d, e, f, g, etc., ω, rangés en cercle et formant ainsi les sommets d'un polygone régulier de N côtés, et supposons que x désigne un nombre quelconque inférieur et premier à N. Prenez ces sommets à partir de l'un quelconque d'entre eux, en les joignant de x en x, ce qui vous donnera un second polygone régulier de N côtés. De ce second polygone tirez-en un troisième, en y prenant encore les lettres de x en x; et de celui-ci, par la même loi, un quatrième, et ainsi de suite, jusqu'à ce que vous retombiez sur le premier polygone d'où vous êtes parti; vous aurez formé ainsi un certain nombre n' de polygones tous différents. Or, où ces polygones feront

tous ceux qu'on peut former en joignant les sommets par tous les intervalles possibles inférieurs et premiers à N, et alors on aura

$$n' = n;$$

ou bien ils n'en feront qu'une partie, et alors je dis que cette partie sera une aliquote de n, de sorte qu'on aura

$$n'\theta = n.$$

En effet, prenez un des n polygones qui n'existe pas dans le groupe des n' polygones différents que vous avez formés, et tirez-en, par la même loi que tout à l'heure, n' polygones réguliers; il est clair d'abord qu'ils seront tous différents entre eux; et ensuite, il est aisé de voir qu'ils seront tous différents des premiers, car si un seul polygone de ce second groupe pouvait revenir à l'un de ceux qui sont dans le premier, comme on déduit toujours par la même loi, le groupe entier reviendrait nécessairement au premier, ce qui est impossible puisqu'on y part d'un polygone qui n'est point dans le premier groupe par hypothèse. On démontrera de même, s'il reste encore d'autres polygones réguliers, qu'il y en aura n' nouveaux, et ainsi de suite jusqu'à ce qu'il n'en reste plus. Et comme il n'y a en tout que n polygones différents de N côtés, il en résulte que le nombre n' de ceux qu'on assemble en prenant les sommets de x en x est nécessairement une partie aliquote du nombre n.

12. Or, il est évident que si dans un polygone on prend les sommets de x en x, et que dans le polygone qui en résulte, on prenne encore de x en x, et ainsi de suite, ce procédé revient au même que que si l'on tirait directement tous les polygones du seul premier, mais en y prenant les sommets : 1° de x en x; 2° de x^2 en x^2; 3° de x^3 en x^3, etc., et enfin de $x^{n'}$ en $x^{n'}$. Mais, par hypothèse, en prenant les sommets de $x^{n'}$ en $x^{n'}$, on retombe sur le polygone même d'où l'on est parti comme si l'on y eût pris simplement les sommets de 1 en 1 : donc l'intervalle $x^{n'}$ par lequel on saute d'un point à l'autre, revient à l'unité relativement au nombre N, c'est-à-dire est égal à 1 plus un multiple de N; de sorte que l'on a

$$x^{n'} = 1 + \mathfrak{M}N.$$

Or, puisque $x^{n'}$ revient à l'unité, il est évident qu'une puissance quelconque de $x^{n'}$ revient aussi à l'unité; donc $(x^{n'})^{\theta}$, ou x^n, revient à 1 relativement à N, c'est-à-dire qu'on a toujours l'équation

$$x^n - 1 = \mathfrak{M}N,$$

quel que soit le nombre entier x premier à N; *ce qu'il fallait démontrer*.

Ainsi l'on a de ce beau théorème une démonstration puisée dans les premiers principes de la chose, et rendue, pour ainsi dire, sensible par la considération des divers polygones réguliers d'un même nombre de côtés. Cette idée simple de passer, par la même loi, d'un polygone à l'autre, en y marchant toujours par le même intervalle, nous mène directement à l'idée des *puissances*, des *résidus*, des *multiples racines* de l'unité, etc. D'où il paraît, comme je l'ai déjà remarqué dans d'autres Mémoires, que la théorie de l'ordre est la source naturelle des propriétés des nombres, et des principes fondamentaux de l'analyse : vérités qui recevront sans cesse un plus grand jour.

13. En attendant, nous pouvons encore démontrer de la même manière que si a, b, c, d, etc., N $-$ 1 sont les n nombres inférieurs et premiers à un nombre quelconque N, l'un ou l'autre des deux nombres

$$1 . a . b\ c . d \text{ etc. } \overline{N - 1} \pm 1$$

est toujours divisible par N.

En effet, soient N lettres rangées en cercle et marquant les angles d'un polygone régulier de N côtés. Prenez les angles de a en a, et comme a est premier à N, vous formerez un second polygone régulier de N côtés. Actuellement, dans ce second polygone, il est évident que vous pouvez prendre les lettres de x en x, de manière à retomber sur le premier polygone; mais, par ces deux opérations, vous aurez pris les lettres de ax en ax; donc, puisque vous retombez sur le premier polygone, prendre les lettres de ax en ax revient à les prendre de 1 en 1.

Donc, si a est premier à N, il y a toujours un autre nombre x aussi premier à N et qui est tel que

$$ax = \mathfrak{M}N + 1.$$

14. Mais il peut arriver que le nombre x soit encore le même que a, alors on aurait

$$a^2 = \mathfrak{M}N + 1.$$

Dans ce cas, prenez les lettres de a en a, comme ci-dessus; mais dans le second polygone qui en résulte, au lieu de les prendre encore de a en a pour retomber sur le premier, prenez de $N - a$ en $N - a$, et vous retomberez sur le premier polygone *renversé*, et par conséquent, vous aurez le produit $a(N - a)$ qui reviendra à -1, c'est-à-dire qu'on aura

$$a \times \overline{N - a} = \mathfrak{M}N - 1.$$

Donc, dans tous les cas, les nombres

$$1,\ a,\ b,\ c,\ d,\ \text{etc.},\ N - 1$$

peuvent toujours s'associer deux à deux de maniere que leur produit revienne à ± 1; donc aussi le produit total $a.b.c.d$ etc. $N - 1$ reviendra nécessairement à ± 1, c'est-à-dire sera de la forme $\mathfrak{M}N \pm 1$; *ce qu'il fallait démontrer.*

15. Quand N est un nombre premier p ou une puissance $m^{ième}$ d'un nombre premier p supérieur à 2, vous ne pouvez jamais trouver que les nombres 1 et $N - 1$ qui soient tels que leurs carrés reviennent à l'unité; sans quoi vous auriez

$$x^2 - 1 = (x + 1)(x - 1)$$

divisible de plus de deux manières par p ou p^m, ce qui ne se peut, puisque, $x + 1$ et $x - 1$ ne pouvant avoir au plus que le commun diviseur 2, vous ne pouvez rendre le produit de ces binômes divisible par p ou p^m qu'en faisant, ou $x + 1 = \mathfrak{M}N$, ou $x - 1 = \mathfrak{M}N$, ce qui ne peut donner que deux valeurs de x au-dessous de N : ainsi, quand $N = p$ ou p^m, on a l'équation

$$a.b.c.d... = \mathfrak{M}N + 1,$$

puisque ces nombres a, b, c, etc., s'associent toujours deux à deux, de manière que le produit revient à $+1$; donc, en multipliant par 1 et

N — 1, on aura

$$1.a.b.c.d...\overline{N-1} = \mathfrak{M}N - 1,$$

ou

$$1.a.b.c.d...\overline{N-1} + 1 = \mathfrak{M}N.$$

On ferait voir la même chose pour le cas de $N = 2p^m$ (p étant > 2).

Solutions nouvelles de l'équation indéterminée du premier degré à deux inconnues.

16. De cette même considération de l'ordre on peut tirer une solution nouvelle, et en quelque sorte *géométrique*, de l'équation indéterminée du premier degré à deux inconnues x et y. Cette solution n'est, en effet, qu'un corollaire de la proposition énoncée plus haut à la fin du n° **13**, mais il n'est pas inutile d'en présenter ici la démonstration expresse.

La forme générale de l'équation indéterminée dont il s'agit est, comme on sait,

$$Lx - My = N,$$

où l'on doit supposer les deux coefficients L et M premiers entre eux; car s'ils avaient un commun diviseur θ autre que l'unité, il faudrait que N fût aussi divisible par θ, sans quoi l'équation serait évidemment impossible en nombres entiers x et y. Si donc l'équation est possible, le plus grand commun diviseur des deux coefficients de x et y divise toute l'équation; de sorte qu'en le supprimant, on a une autre équation équivalente où les nouveaux coefficients L et M sont premiers entre eux. Il suffit même de résoudre la simple équation

$$Lx - My = 1,$$

parce que si l'on en trouve les racines x et y, on n'aura qu'à les multiplier par N, ce qui donnera Nx et Ny pour les racines de la proposée.

Première solution.

17. Soit donc à résoudre l'équation indéterminée

$$Lx - My = 1,$$

et supposons, par exemple, qu'on veuille avoir d'abord la valeur de x.

Je prends une suite de points

$$a\ b\ c\ d\ e\ f\ g \ldots\ \omega,$$

en nombre M coefficient de l'autre inconnue y; et, à partir du premier point a, je joins ces points, non pas de suite, mais en sautant de l'un à l'autre par l'intervalle constant L qui est le coefficient de x; et comme L est premier à M par hypothèse, je passe nécessairement par tous les points avant de retomber sur le point de départ, et je forme ainsi un nouvel ordre ou polygone du même nombre M de sommets. Or, si dans ce nouvel ordre je joignais les points en allant de l'un à l'autre par l'intervalle λ qui y sépare a de b, il est clair que je retomberais sur le premier ordre $a\ b\ c\ d\ e\ f\ldots$, comme si dans ce premier ordre j'avais pris simplement les points de suite ou de 1 en 1. Donc, puisque la double opération d'aller de L en L dans le premier ordre, et puis de λ en λ dans le second, revient à marcher tout d'un coup de $L\lambda$ en $L\lambda$, le produit $L\lambda$ revient à l'unité relativement au nombre M. c'est-à-dire qu'on a

$$L\lambda = 1 \textit{ plus un certain multiple de } M,$$

et par conséquent

$$x = \lambda$$

pour la plus petite valeur de x qui satisfasse à la proposée; et de là on tirerait sur-le-champ

$$y = \frac{L\lambda - 1}{M} = \mu$$

pour la plus petite valeur μ de y, conjuguée à cette valeur λ de x.

Au reste, il est clair qu'on pourrait trouver la valeur de y aussi directement que celle de x, en considérant un polygone de L sommets $a\ b\ c\ d\ldots\ \omega$, et les joignant de M en M coefficient de y; ce qui donnerait un nouvel ordre de ces L sommets. Car, dans ce nouvel ordre, si l'on prenait l'intervalle μ qui y sépare a, non pas de b qui suivait a dans l'ordre primitif, mais de ω qui l'y précédait, il est clair qu'on retomberait sur le polygone renversé $a\ \omega\ldots\ e\ d\ c\ b$, comme si l'on avait marché de -1 en -1 dans l'ordre primitif. Donc μ sera la plus

petite valeur de y qui résoudrait l'équation

$$My - Lx = -1,$$

et par conséquent l'équation

$$Lx - My = 1,$$

qui est la proposée même.

Connaissant les deux plus petits nombres λ et μ qui satisfont ensemble à la proposée, on aura, pour toutes les autres valeurs possibles de x et y qui jouissent de la même propriété,

$$x = \lambda + iM,$$
$$y = \mu + iL;$$

i étant un nombre entier quelconque, positif ou négatif, mais qu'on doit toujours prendre le même dans les deux expressions.

Exemple.

18. Pour éclaircir la règle par une application très-simple, soit, par exemple, à résoudre l'équation indéterminée

$$12x - 7y = 1;$$

je prends 7 points dans l'ordre

$$a\ b\ c\ d\ e\ f\ g,$$

et de cet ordre, en y allant de 12 en 12, ou, ce qui revient au même, de 5 en 5 (à cause de $12 = 5$ à un multiple près de 7), je tire l'ordre nouveau

$$a\ f\ d\ b\ g\ e\ c,$$

où je vois que l'intervalle qui sépare a de b est 3; que par conséquent le plus petit nombre x qui satisfait à la proposée est $x = 3$: et de là, par la proposée même, je tirerais tout de suite $y = 5$ pour la plus petite valeur de y conjuguée à la valeur de x.

Si l'on avait voulu trouver directement y, on aurait pris une suite de points

$$a\ b\ c\ d\ e\ f\ g\ h\ i\ k\ l\ m,$$

au nombre de 12, coefficient de l'autre inconnue x; et, les joignant de 7 en 7, on aurait trouvé l'ordre nouveau

$$a\ h\ c\ k\ e\ m\ g\ b\ i\ d\ l\ f,$$

où l'on voit que la distance qui sépare a, non pas de b qui le suivait dans l'ordre primitif, mais bien de m qui l'y précédait, est égale au nombre 5 : d'où résulte $y = 5$ pour la plus petite valeur de y qui résoudrait l'équation

$$7y - 12x = -1,$$

ou, en changeant les signes,

$$12x - 7y = 1,$$

qui est la proposée même.

On peut faire d'autres exemples, et l'on trouvera que la méthode est assez prompte, pourvu qu'un des deux coefficients L et M soit un nombre peu considérable. Car, en se bornant alors à ne chercher, par cette voie, que l'inconnue affectée du grand coefficient, on n'aura besoin de marquer des points $a, b, c, \ldots, \omega$, qu'en nombre égal au plus petit, ce qui fera connaître la première inconnue; après quoi l'on pourra tirer l'autre de l'équation même. Mais si les coefficients étaient tous deux un peu grands, il faudrait ranger par ordre beaucoup de points $a, b, c, d, e, \ldots, \omega$, ce qui serait long et fastidieux, ou même impraticable. Toutefois la solution n'en est pas moins curieuse dans la théorie, par les rapprochements qu'on en peut faire avec les solutions arithmétiques déjà connues.

Seconde solution.

19. Au reste, on peut encore déduire du théorème donné au n° **11**, une nouvelle solution de l'équation indéterminée

$$Lx - My = 1.$$

Car, dans le polygone de M côtés, joignez les sommets de L en L, ce qui donne un deuxième polygone : dans celui-ci, joignez encore de L en L, ce qui donnera un troisième polygone; et continuez ainsi jusqu'à l'opération $m^{ième}$ qui vous fera retomber sur le polygone primitif.

Comme le résultat de ces m opérations sera le même que si vous aviez marché tout d'un coup de L^m en L^m, il s'ensuit que l'intervalle L^m revient à l'unité relativement à M. Donc, pour trouver x, au lieu d'écrire que Lx doit revenir à 1, vous pouvez écrire que Lx doit revenir à L^m, et alors il est évident que x revient à L^{m-1}.

Ainsi la plus petite valeur de x peut se trouver en formant le $m-1^{ième}$ polygone dérivé, y prenant deux sommets consécutifs, et regardant à quelle distance ces deux sommets se trouvent l'un de l'autre dans le polygone primitif; cette distance sera le nombre cherché x.

Voilà donc, en apparence, une seconde solution géométrique de l'équation indéterminée

$$Lx - My = 1;$$

mais il est aisé de voir que cette solution (abrégée comme elle peut l'être) ne diffère point de celle qu'on a donnée plus haut. Car ici le polygone primitif pouvant être regardé comme étant le $m^{ième}$ dérivé, et par conséquent comme celui qui vient après le $m-1^{ième}$, il est clair que les deux polygones qu'on emploie ici pour avoir x sont deux polygones dérivés *consécutifs*. Or, puisque tous nos polygones naissent l'un de l'autre par la même loi, on peut employer de même deux autres polygones consécutifs *quelconques*, tels que le premier et le second; ce qui nous ramène précisément à la solution géométrique du n° 17.

20. Mais, en arithmétique, l'expression

$$x = L^{m-1}$$

nous donne cette règle nouvelle pour trouver x : *Faites les puissances successives* L, L^2, L^3, *etc., en rabaissant à mesure au-dessous de* M *par la division,* et continuez ainsi jusqu'à ce que vous trouviez le reste 1; le reste précédent sera la plus petite valeur de x qui résout la proposée

$$Lx - My = 1.$$

Quant à cette puissance m jusqu'à laquelle il faudra monter pour obtenir $L^m = 1$, elle dépend des nombres M et L. Si l'on désigne par μ le nombre qui marque combien il y a de nombres L inférieurs et premiers à M, on peut dire, en général, que m sera toujours une

aliquote du nombre μ, et cette aliquote ne pourra s'élever jusqu'au nombre μ lui-même que dans le cas où M serait un nombre premier, ou une puissance de nombre premier, ou le double d'une telle puissance; et, même dans ces cas, on n'aura $m = \mu$ que pour autant de nombres L qu'il y aura de nombres inférieurs et premiers à μ. Dans tous les autres cas, m sera inférieur à μ; il en sera tel ou tel sous-multiple, suivant la nature du nombre L comparé au module M.

On trouverait de même, pour l'expression directe de l'autre inconnue y,

$$y = -(M^{l-1}),$$

l étant la puissance de M qui donnera $M^l = 1$, relativement au module L; etc., etc.

CHAPITRE IV.

Théorie des équations binômes.

Je reviens ici à la théorie des équations binômes, et je vais chercher les propriétés de leurs racines par la forme même de ces équations.

Article Ier.

Des équations binômes rapportées à un module premier p.

1. Soit l'équation binôme indéterminée $x^n - 1 = \mathfrak{M}p$, et désignons par r une quelconque des racines de cette équation.

Je dis d'abord qu'*on ne peut avoir en même temps*

$$r^n = 1 + \mathfrak{M}p, \quad et \quad r^h = 1 + \mathfrak{M}p,$$

à moins qu'on n'ait aussi

$$r^\theta = 1 + \mathfrak{M}p,$$

θ étant le plus grand commun diviseur de n et h.

Car soit i le reste de la division de n par h, de manière qu'on ait

$$n = hq + i,$$

il est clair que des deux équations supposées, on tirerait

$$r^i = 1 + \mathfrak{M} p;$$

et, en effet, la première pourrait se mettre sous la forme

$$r^{hq+i} = 1 + \mathfrak{M} p, \quad \text{ou} \quad (r^h)^q \times r^i = 1 + \mathfrak{M} p;$$

mais, à cause de la seconde équation

$$r^h = 1 + \mathfrak{M} p,$$

le facteur $(r^h)^q$ revient à $1 + \mathfrak{M} p$; donc l'équation

$$(r^h)^q \times r^i = 1 + \mathfrak{M} p$$

reviendrait à

$$r^i = 1 + \mathfrak{M} p.$$

Mais, pareillement, des deux équations

$$r^h = 1 + \mathfrak{M} p, \quad \text{et} \quad r^i = 1 + \mathfrak{M} p,$$

on tirerait

$$r^{i'} = 1 + \mathfrak{M} p,$$

i' étant le reste de la division de h par i, et ainsi de suite : d'où il résulte qu'on aurait enfin

$$r^\theta = 1 + \mathfrak{M} p,$$

θ étant le plus grand commun diviseur de n et h.

Cette démonstration est tout à fait la même que celle qu'on ferait pour prouver que les deux binômes $x^n - 1$ et $x^h - 1$ ne peuvent avoir de commun diviseur plus élevé que le binôme $x^\theta - 1$, θ étant le plus grand commun diviseur de n et h.

2. Si n et h sont premiers entre eux, c'est-à-dire si $\theta = 1$, les deux équations

$$x^n - 1 = \mathfrak{M} p, \quad \text{et} \quad x^h - 1 = \mathfrak{M} p,$$

ne peuvent avoir d'autre racine commune que l'unité.

Mais, en vertu du théorème de Fermat, l'équation

$$x^{p-1} - 1 = \mathfrak{M} p$$

a toujours $p-1$ racines entieres inférieures à p, et ces racines font ainsi tous les nombres de la suite naturelle $1, 2, 3, 4, 5, ..., p-1$. Donc aucune équation

$$x^n - 1 = \mathfrak{M}\, p$$

ne peut avoir de racines entières autres que l'unité, à moins qu'il n'y ait entre n et $p-1$ un commun diviseur θ autre que l'unité.

3. Si n est premier à $p-1$, $x^n - 1 = \mathfrak{M}\, p$ n'a donc aucune autre racine réelle que l'unité.

Si entre n et $p-1$, il y a le plus grand commun diviseur $\theta > 1$, $x^n - 1 = \mathfrak{M}\, p$ aura nécessairement, parmi les nombres $1, 2, 3, 4, 5, ..., p-1$, θ racines réelles. Car le binôme $x^\theta - 1$ sera un diviseur rationnel de $x^{p-1} - 1$, et par conséquent sera divisible par p pour θ valeurs de x inférieures à p.

Lors donc que l'on considère une équation binôme indéterminée

$$x^n - 1 = \mathfrak{M}\, p,$$

il n'y a pas d'autres racines réelles à chercher que celles qui conviennent à

$$x^\theta - 1 = \mathfrak{M}\, p,$$

θ étant le plus grand commun diviseur de n et $p-1$. Il est donc inutile de considérer d'autres équations

$$x^n - 1 = \mathfrak{M}\, p,$$

que celles où l'exposant n est un diviseur de $p-1$.

Si, par exemple, on proposait les équations

$$x^7 - 1 = \mathfrak{M}\, 13, \quad x^{10} - 1 = \mathfrak{M}\, 13, \quad x^{15} - 1 = \mathfrak{M}\, 13, \quad \text{etc.},$$

cela reviendrait à proposer les équations respectives

$$x - 1 = \mathfrak{M}\, 13, \quad x^2 - 1 = \mathfrak{M}\, 13, \quad x^3 - 1 = \mathfrak{M}\, 13, \quad \text{etc.},$$

car ces dernières renferment les seules racines entières que puissent avoir les équations données.

4. Considérez les puissances successives r, r^2, r^3, r^4, etc, de l'une

quelconque des racines r de l'équation

$$x^n - 1 = \mathfrak{M} p;$$

il est clair, par la forme même de l'équation, que toutes ces puissances en seront aussi des racines : car si

$$r^n = 1 + \mathfrak{M} p,$$

on aura aussi

$$(r^2)^n, \quad \text{ou} \quad (r^n)^2 = 1 + \mathfrak{M} p; \qquad (r^3)^n, \quad \text{ou} \quad (r^n)^3 = 1 + \mathfrak{M} p;$$

et, en général,

$$(r^e)^n, \quad \text{ou} \quad (r^n)^e = 1 + \mathfrak{M} p.$$

Or, actuellement, je dis que deux quelconques de ces puissances r^e, $r^{e'}$ ne pourront être équivalentes, c'est-à-dire donner un même reste relativement à p, à moins que la racine r qu'on aura employée ne soit en même temps racine d'une équation inférieure

$$x^d - 1 = \mathfrak{M} p,$$

d étant un diviseur de l'exposant n.

Et, en effet, soit $e > e'$, e et e' étant d'ailleurs au-dessous de n. Si l'on avait

$$r^e - r^{e'} = \mathfrak{M} p,$$

on en tirerait

$$r^{e'} (r^{e-e'} - 1) = \mathfrak{M} p;$$

mais le facteur $r^{e'}$ n'étant pas divisible par p, puisque r est premier à p, il faudrait que l'autre facteur $r^{e-e'} - 1$ fût divisible par p, et partant, qu'on eût, en faisant $e - e' = h$,

$$r^h - 1 = \mathfrak{M} p;$$

mais cette équation ne peut avoir lieu en même temps que la proposée, à moins que h n'ait un commun diviseur d avec n, et par conséquent à moins que r ne soit une racine de l'équation binôme de degré inférieur

$$x^d - 1 = \mathfrak{M} p.$$

Article II.

Des racines primitives de l'équation $x^n - 1 = \mathfrak{M} p$.

5. Imaginez donc qu'on prenne pour r une racine de

$$x^n - 1 = \mathfrak{M} p,$$

mais qui n'appartienne pas en même temps à une autre équation binôme

$$x^d - 1 = \mathfrak{M} p$$

de degré inférieur d, diviseur de n; alors toutes les puissances r, r^2, r^3, $r^4, \ldots, r^n$, de cette racine r, seront différentes relativement à p, et par conséquent cette racine r sera propre à former par ses puissances successives la suite complète de toutes les racines de la proposée. Ce sera ce qu'on peut appeler une *racine primitive* de l'équation

$$x^n - 1 = \mathfrak{M} p,$$

c'est-à-dire une racine uniquement propre à cette équation.

Si l'exposant n est un nombre premier, on voit tout de suite que cette racine primitive existe, et même que toutes les racines de

$$x^n - 1 = \mathfrak{M} p,$$

autres que l'unité, sont des racines primitives : car aucune d'elles ne peut appartenir à aucune équation inférieure

$$x^d - 1 = \mathfrak{M} p,$$

puisque n, étant premier, ne peut avoir d'autre diviseur d que l'unité.

6. Ainsi, quand n est un nombre premier, toutes les racines de

$$x^n - 1 = \mathfrak{M} p,$$

autres que l'unité, sont uniquement propres à cette équation, c'est-à-dire ne résolvent aucune équation binôme de degré inférieur à n; chacune d'elles, par ses puissances successives 1, 2, 3, 4, 5, 6,..., n, fournit la suite complète de toutes les racines différentes de la proposée; elle ne donne l'unité qu'à la puissance $n^{ième}$; après quoi toutes les racines reparaissent périodiquement dans le même ordre à l'infini.

Mais quand l'exposant n est un nombre composé, il n'y a plus qu'une partie des racines qui soient uniquement propres à l'équation

$$x^n - 1 = \mathfrak{M}\,p,$$

ou qui en soient des racines primitives; car les autres résolvent en même temps des équations binômes de degrés inférieurs marqués par les différents diviseurs de n; de sorte que leurs puissances successives ramènent l'unité avant la puissance $n^{ième}$, et ne peuvent ainsi former la suite complète des n racines différentes de la proposée.

De l'existence des racines primitives et de leur nombre.

7. Voyons donc d'abord si l'équation $x^n - 1 = \mathfrak{M}\,p$ a toujours des racines primitives, quel que soit le nombre n, et combien il y a de ces racines.

Nous avons déjà remarqué que, pour un exposant a premier, il y a $a - 1$ racines primitives; et, en effet, l'exposant a n'ayant pas d'autre diviseur que l'unité, le binôme $x^a - 1$ n'a pas d'autre diviseur binôme de degré inférieur, que le binôme $x - 1$. Ainsi toutes les racines de

$$x^a - 1 = \mathfrak{M}\,p,$$

excepté la racine $x = 1$, sont uniquement propres à cette équation, et, comme on l'a dit, en sont des racines primitives.

Si l'on a $n = a^2$, a étant toujours un nombre premier, l'exposant n n'a pas au-dessous de lui de plus grand diviseur que a, et par conséquent, le binôme $x^{a^2} - 1$ n'a pas, au-dessous de lui, de diviseur binôme plus élevé que $x^a - 1$. En rejetant donc de la proposée les a racines de l'équation

$$x^a - 1 = \mathfrak{M}\,p,$$

il en restera $a^2 - a$ qui seront uniquement propres à l'équation

$$x^{a^2} - 1 = \mathfrak{M}\,p.$$

Si l'on a $n = a^3$, on trouvera de même qu'en rejetant les a^2 racines de l'équation

$$x^{a^2} - 1 = \mathfrak{M}\,p,$$

on aura rejeté toutes celles qui peuvent résoudre les équations binômes de degrés inférieurs, et que, par conséquent, il en reste $a^3 - a^2$ qui sont uniquement propres à la proposée

$$x^{a^3} - 1 = \mathfrak{M} p.$$

En général, soit $n = a^\alpha$, et par conséquent

$$x^{a^\alpha} - 1 = \mathfrak{M} p$$

l'équation proposée. Si l'on rejette les racines de l'équation binôme

$$x^{a^{\alpha-1}} - 1 = \mathfrak{M} p,$$

on aura rejeté toutes celles qui résolvent, en même temps que la proposée, des équations binômes de degrés inférieurs; et, par conséquent, les racines restantes, qui seront au nombre de $a^\alpha - a^{\alpha-1}$, seront toutes des racines primitives.

Ainsi, pour un exposant n qui est une puissance quelconque α d'un nombre premier a, l'équation

$$x^n - 1 = \mathfrak{M} p$$

a toujours des racines primitives; et le nombre en est

$$a^\alpha - a^{\alpha-1}, \quad \text{ou} \quad a^{\alpha-1}(a-1),$$

c'est-à-dire qu'il y en a autant que de nombres inférieurs et premiers à n (n° 7, chap. II).

8. Ce théorème est général pour un nombre quelconque n; et d'abord il serait bien facile de le reconnaître pour le cas de $n = a^\alpha b^6$, a et b étant deux nombres premiers quelconques. Car de l'équation

$$x^{a^\alpha b^6} - 1 = \mathfrak{M} p,$$

qui a un nombre $a^\alpha b^6$ de racines, imaginez qu'on rejette les $a^{\alpha-1} b^6$ racines de l'équation inférieure

$$x^{a^{\alpha-1} b^6} - 1 = \mathfrak{M} p,$$

et puis les $a^\alpha b^{6-1}$ racines de l'équation inférieure

$$x^{a^\alpha b^{6-1}} - 1 = \mathfrak{M} p;$$

il est évident qu'on aura rejeté toutes les racines qui peuvent résoudre des équations binômes de degrés inférieurs à la proposée et diviseurs de n. Ainsi l'on trouverait d'abord qu'il doit rester

$$a^{\alpha\beta} - a^{\alpha-1}b^{\beta} - a^{\alpha}b^{\beta-1}$$

racines; mais ce nombre est trop faible: car, par la double opération précédente, il est clair qu'on a ôté deux fois les racines communes aux deux équations

$$x^{a^{\alpha-1}b^{\beta}} - 1 = \mathfrak{M}p, \quad x^{a^{\alpha}b^{\beta-1}} - 1 = \mathfrak{M}p,$$

racines communes qui sont au nombre de $a^{\alpha-1}b^{\beta-1}$; donc, au résultat précédent, il faut ajouter $a^{\alpha-1}b^{\beta-1}$, et l'on trouve ainsi, pour le nombre des racines qui appartiennent uniquement à la proposée,

$$a^{\alpha}b^{\beta} - a^{\alpha-1}b^{\beta} - a^{\alpha}b^{\beta-1} + a^{\alpha-1}b^{\beta-1},$$

ce qui se réduit à

$$a^{\alpha-1}b^{\beta-1}(a-1)(b-1);$$

d'où l'on voit qu'il y a encore autant de racines primitives que de nombres inférieurs et premiers à n.

La même démonstration pourrait s'étendre au cas de $n = a^{\alpha}b^{\beta}c^{\gamma}\ldots$; mais nous allons présenter la chose d'une manière plus claire, et qui peut même servir à trouver les racines primitives.

9. Soit donc, en général, $n = a^{\alpha}b^{\beta}c^{\gamma}\ldots$ et l'équation binôme

$$x^{a^{\alpha}b^{\beta}c^{\gamma}\ldots} - 1 = \mathfrak{M}p.$$

Je considère les équations

$$x^{a^{\alpha}} - 1 = \mathfrak{M}p, \quad x^{b^{\beta}} - 1 = \mathfrak{M}p, \quad x^{c^{\gamma}} - 1 = \mathfrak{M}p, \ldots,$$

et je suppose que x' soit une racine primitive de la première, x'' une racine primitive de la seconde, x''' une racine primitive de la troisième, etc.; alors je dis que le produit $x'x''x'''\ldots$ est une racine primitive de la proposée. En effet, il est clair, en premier lieu, que ce produit est racine de l'équation

$$x^{n} - 1 = \mathfrak{M}p;$$

c'est-à-dire qu'étant élevé à la puissance $n = a^\alpha b^\beta c^\gamma \ldots$, il donne $1 + \mathfrak{M}\, p$, ou simplement 1, en négligeant les multiples de p. Mais, en second lieu, il est aisé de voir qu'il ne peut donner l'unité pour aucune puissance d inférieure à n: car si l'on avait

$$(x' x'' x''' \ldots)^d = 1 + \mathfrak{M}\, p,$$

l'exposant d serait nécessairement diviseur de n (n° 4); mais d étant plus petit que n, il y a au moins quelque facteur simple de n, tel que a, je suppose, qui entre une fois de moins dans le nombre d que dans le nombre n; ainsi d serait diviseur de $a^{\alpha-1} b^\beta c^\gamma \ldots$; donc, puisque $x' x'' x''' \ldots$ élevé à la puissance d donne 1, ce même produit à la puissance $a^{\alpha-1} b^\beta c^\gamma \ldots$ qui est multiple de d, donnerait aussi 1; donc on aurait

$$(x' x'' x''' \ldots)^{a^{\alpha-1} b^\beta c^\gamma \ldots} = 1 + \mathfrak{M}\, p:$$

mais, à cause de

$$x''^{b^\beta} = 1 + \mathfrak{M}\, p, \quad x'''^{c^\gamma} = 1 + \mathfrak{M}\, p, \quad \text{etc.},$$

cette équation se réduit à

$$x'^{a^{\alpha-1} b^\beta c^\gamma \ldots} = 1 + \mathfrak{M}\, p;$$

or, par hypothèse, on a

$$x'^{a^\alpha} = 1 + \mathfrak{M}\, p;$$

donc on aurait aussi, en prenant le commun diviseur $a^{\alpha-1}$ des deux exposants de ces équations (n° 3),

$$x'^{a^{\alpha-1}} = 1 + \mathfrak{M}\, p;$$

donc x' donnerait l'unité avant la puissance a^α, et partant, ne serait pas racine primitive de l'équation

$$x^{a^\alpha} - 1 = \mathfrak{M}\, p,$$

ce qui est contre l'hypothèse.

Donc le produit $x' x'' x''' \ldots$ ne peut donner l'unité pour aucune puissance d inférieure à $a^\alpha b^\beta c^\gamma \ldots$; donc il est racine primitive de l'équation proposée

$$x^{a^\alpha b^\beta c^\gamma \ldots} - 1 = \mathfrak{M}\, p.$$

Ce qu'il fallait démontrer.

Ainsi donc, toute équation

$$x^n - 1 = \mathfrak{M}\,p$$

a des racines primitives, et le nombre en est au moins égal à celui de tous les produits différents $x'x''x'''\ldots$ qu'on peut faire en combinant les racines primitives x', x'', x''',... des équations respectives

$$x^{a^\alpha} - 1 = \mathfrak{M}\,p, \quad x^{b^6} - 1 = \mathfrak{M}\,p, \quad x^{c^\gamma} - 1 = \mathfrak{M}\,p, \quad \text{etc.};$$

or, le nombre des racines primitives x' de la première équation est $a^{\alpha-1}(a-1)$; les racines primitives x'' de la deuxième sont au nombre de $b^{6-1}(b-1)$; les racines primitives x''' de la troisième sont au nombre de $c^{\gamma-1}(c-1)$, etc.: donc, par la théorie des combinaisons, les racines primitives de la proposée

$$x^n - 1 = x^{a^\alpha b^6 c^\gamma \ldots} - 1 = \mathfrak{M}\,p$$

sont au moins au nombre de

$$a^{\alpha-1}(a-1).b^{6-1}(b-1).c^{\gamma-1}(c-1)\ldots,$$

c'est-à-dire qu'il y en a au moins autant que de nombres inférieurs et premiers à n; et il est bien aisé de voir qu'il n'y en a pas davantage.

10. Au reste, dès qu'on suppose l'existence d'une seule racine primitive de

$$x^n - 1 = \mathfrak{M}\,p,$$

on peut démontrer tout de suite qu'il y en a précisément le nombre qu'on vient de dire. Car, soit r cette racine primitive, et formez la suite des puissances

$$r,\ r^2,\ r^3,\ r^4,\ r^5,\ r^6,\ldots,\ r^{n-1},\ r^n;$$

il est clair qu'on aura la suite complète des n racines différentes de la proposée; or, si l'on considère un nombre quelconque e inférieur et premier à n, et qu'on prenne les racines dans cette même suite, en allant de l'un à l'autre de e en e; comme l'intervalle e par lequel on saute est premier à n, on sera obligé de passer par toutes les racines avant de revenir à la racine r d'où l'on est parti; donc la suite

$$r^e,\ (r^e)^2,\ (r^e)^3,\ (r^e)^4,\ldots,\ (r^e)^n$$

nous donne aussi, aux multiples près de p, toutes les différentes racines de la proposée : donc r^e est aussi racine primitive.

Donc, si l'on suppose une seule racine primitive r de l'équation

$$x^n - 1 = \mathfrak{M}p,$$

il s'ensuit qu'il y en a autant que de nombres e inférieurs et premiers à n. Et l'on voit en même temps qu'il n'y en a pas davantage : car si l'on va d'une racine à l'autre, par un intervalle constant h qui ait avec n un commun diviseur $\theta > 1$, on ne passera jamais que par un nombre $\frac{n}{\theta}$ de ces racines ; de sorte que r^h ne peut jamais être racine primitive de

$$x^n - 1 = \mathfrak{M}p.$$

Mais il est évident, par la même démonstration, que r^h sera racine primitive de l'équation inférieure

$$x^{\frac{n}{\theta}} - 1 = \mathfrak{M}p.$$

11. On voit ici se présenter tout naturellement l'idée et la raison du théorème établi au n° **18** du chapitre II, mais qui paraissait un peu isolé.

En effet, je remarque que de toutes les racines de l'équation

$$x^n - 1 = \mathfrak{M}p,$$

il n'y en a pas une seule qui ne soit racine primitive, ou de la proposée, ou de quelque autre équation inférieure

$$x^d - 1 = \mathfrak{M}p,$$

d étant un diviseur de n. Car prenez au hasard une racine ρ de

$$x^n - 1 = \mathfrak{M}p,$$

et faites-en les puissances successives ρ, ρ^2, ρ^3, ρ^4,..., vous tomberez nécessairement sur quelque puissance ρ^d qui vous donnera l'unité relativement à p, et alors ρ sera racine primitive de l'équation

$$x^d - 1 = \mathfrak{M}p.$$

De plus, on voit que ρ ne peut être racine primitive d'aucune autre équation semblable d'un degré marqué par un autre diviseur de n.

Or, cette équation

$$x^d - 1 = \mathfrak{M}p$$

a autant de racines primitives qu'il y a de nombres inférieurs et premiers à d; donc, si l'on voulait compter combien il y a en tout de nombres inférieurs et premiers à chacun de tous les diviseurs possibles d d'un nombre donné n, sans excepter le diviseur 1 et le nombre n lui-même, on trouverait qu'il y en a autant que l'équation

$$x^n - 1 = \mathfrak{M} p$$

a de racines, c'est-à-dire précisément n. Ce qui est le théoreme dont il s'agit.

12. Mais, réciproquement, de ce dernier théorème, qui est d'ailleurs démontré d'une *manière directe*, on peut conclure l'existence des racines primitives de toute équation

$$x^n - 1 = \mathfrak{M} p.$$

Car, en considérant toutes les racines qui sont au nombre de n, s'il n'y en avait point de primitives, c'est-à-dire qui fussent uniquement propres à cette équation, il faudrait donc qu'elles fussent toutes les racines propres à des équations inférieures

$$x^d - 1 = \mathfrak{M} p$$

dont les degrés seraient les différents diviseurs d de n, le nombre n étant excepté de ces diviseurs. Mais chaque équation

$$x^d - 1 = \mathfrak{M} p$$

ne peut avoir plus de racines primitives qu'il n'y a de nombres inférieurs et premiers à d; donc vous ne pourriez jamais compter plus de racines différentes qu'il n'y a de nombres inférieurs et premiers à chacun des diviseurs de n, le nombre n étant excepté; or cela ferait nécessairement un nombre moindre que n, puisque vous n'en trouveriez que n, en n'omettant aucun diviseur. Donc, puisque l'équation

$$x^n - 1 = \mathfrak{M} p$$

a n racines, vous ne pouvez pas supposer qu'elles appartiennent toutes à des équations binômes de degrés inférieurs d diviseurs de n; donc il y en a quelques-unes qui appartiennent uniquement à l'équation

$$x^n - 1 = \mathfrak{M} p;$$

et dès qu'on en suppose une seule, il est clair (n° **10**) qu'il y en a autant que de nombres inférieurs et premiers à n.

13. On voit donc par là, de la manière la plus simple et la plus lumineuse, que toute équation

$$x^n - 1 = \mathfrak{M}p$$

a des racines primitives; qu'une quelconque de ces racines étant nommée r, toutes les autres sont exprimées par r^e, $r^{e'}$, $r^{e''}$,..., les exposants e, e', e'',... étant, après l'unité, tous les nombres inférieurs et premiers à n; enfin, que toute puissance r^h d'exposant h non premier avec n, est simplement une racine primitive de l'équation inférieure

$$x^{\frac{n}{\theta}} - 1 = \mathfrak{M}p,$$

θ étant le plus grand commun diviseur de h et n.

14. Si le nombre n diviseur de $p - 1$ est le nombre $p - 1$ lui-même, on a l'équation $x^{p-1} - 1 = \mathfrak{M}p$, qui répond au théorème de Fermat, et dont les racines primitives s'appellent simplement les racines primitives du nombre premier p.

Comme cette équation renferme toutes les équations semblables

$$x^n - 1 = \mathfrak{M}p,$$

où n est une aliquote de $p - 1$, il s'ensuit qu'il suffit de connaître une seule racine primitive de p, non-seulement pour avoir toutes les autres, comme on vient de le voir, mais encore pour avoir les racines primitives des équations

$$x^n - 1 = \mathfrak{M}p,$$

d'un degré n diviseur de $p - 1$.

Et, en effet, soit a une racine primitive de

$$x^{p-1} - 1 = \mathfrak{M}p, \quad \text{et faisons} \quad \frac{p-1}{n} = h,$$

il est évident que $r = a^h$ sera une racine primitive de l'équation

$$x^n - 1 = \mathfrak{M}p;$$

et de cette racine on conclura toutes les autres.

Article III.

Méthode assez simple pour trouver les racines primitives d'un nombre premier donné.

15. Quant à la manière de trouver les racines primitives d'un nombre premier donné, voici, je crois, la règle la plus simple, et que j'expliquerai d'abord sur un exemple. Supposons qu'il s'agisse, entre autres, du nombre premier $p = 61$.

Comme le nombre inférieur $p - 1$, qui est ici 60, a pour facteurs simples 2, 3 et 5, je remarque que les racines primitives de 61, ou de l'équation

$$x^{60} - 1 = \mathfrak{M}61,$$

ne peuvent être ni des *carrés*, ni des *cubes*, ni des *cinquièmes puissances*. Car, à cause des diviseurs simples 2, 3 et 5 du nombre 60, les carrés étant élevés aux puissances successives 1, 2, 3, 4, etc., rameneraient l'unité au moins dès la trentième puissance; les cubes la rameneraient au moins dès la vingtième, et les autres dès la douzième. Ainsi, pour avoir les racines primitives de 61, c'est-à-dire les nombres qui ne peuvent ramener l'unité avant la soixantième puissance, il suffit d'exclure des soixante nombres de la suite naturelle

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ \text{etc.},\ 60,$$

tous ceux qui sont des carrés, des cubes et des cinquièmes puissances, ou plutôt des résidus de ces puissances par rapport à 61. Or, au moyen des carrés, on exclut d'abord la *moitié* de tous les nombres; au moyen des cubes de ceux qui restent, on en exclut le *tiers*; et par les cinquièmes puissances de ceux qui restent, on en rejette encore le *cinquième*, et il ne reste plus que les seize racines primitives de 61.

Et il est évident qu'il en serait de même pour un nombre premier quelconque p, en excluant des $p - 1$ nombres 1, 2, 3, 4, 5, 6, 7, etc., $p - 1$, les puissances marquées par les facteurs simples 2, a, b, c, etc., du nombre composé $p - 1$. D'où l'on voit encore pourquoi il y a précisément autant de ces racines primitives qu'il y a de nombres inférieurs et premiers à $p - 1$.

Cette règle nous paraît facile, et, dans l'application, on peut diriger

le calcul de manière à ne pas faire plus d'opérations qu'il n'y a de nombres à exclure.

16. Soit, par exemple, à trouver les racines primitives du nombre premier 31.

On voit d'abord qu'il suffit de faire les quinze carrés des nombres 1, 2, 3, 4, etc., 15 : car les autres reviendraient à ceux de — 1, — 2, — 3, etc., — 15, qui donneraient les mêmes carrés.

Supprimant donc dans la suite des trente nombres 1, 2, 3, 4, 5, etc., 30, les quinze nombres qui sont des carrés, il reste les quinze non carrés, dont il faut faire à présent les cubes.

Mais, comme on ne doit trouver que cinq cubes différents, on peut viter les opérations inutiles, en rangeant d'abord les quinze non résidus dans l'ordre où ils suivraient une même raison géométrique. Qu'on prenne, par exemple, la raison 2, et les quinze non résidus pourront s'ordonner de cette manière :

3, 6, 12, 24, 17 | 15, 30, 29, 27, 23 | 13, 26, 21, 11, 22,

où ces non-résidus se trouvent distribués en trois groupes de cinq termes en progression géométrique, et dont les cubes sont :

27, 30, 23, 29, 15 | 27, 30, 23, 29, 15 | 27, 30, 23, 29, 15,

c'est-à-dire les mêmes pour chaque groupe.

Il suffit donc de former les cinq cubes des nombres contenus dans un quelconque des trois groupes.

En supprimant ces cubes, il reste pour les nombres qui ne sont ni carrés, ni cubes,

3, 6, 12, 24, 17 | 13, 26, 21, 11, 22.

Si l'on en fait les cinquièmes puissances, on trouve

26, 26, 26, 26, 26 | 6, 6, 6, 6, 6,

c'est-à-dire qu'il suffisait de faire la cinquième puissance d'un terme pris dans le premier groupe, et celle d'un terme pris dans le second. En effaçant ces deux puissances cinquièmes 26 et 6, il reste les huit racines primitives de 31, savoir :

3, 12, 24, 17, 13, 21, 11, 22.

17. Dans les *Nouveaux Commentaires de Saint-Pétersbourg* (tome XVIII), Euler dit, en plusieurs endroits, qu'on ne voit encore aucun moyen de déterminer ces racines; que la démonstration qui prouve, dans tous les cas, leur existence, n'indique pourtant aucune méthode pour les découvrir : et ailleurs, on ne peut, dit-il, saisir entre un nombre premier et les racines primitives qui lui appartiennent, aucune relation d'où l'on puisse déduire au moins *une seule* de ces racines; de sorte que la loi qui règne entre elles paraît aussi profondément cachée que celle qui peut exister entre les nombres premiers eux-mêmes.

Il nous semble que la méthode précédente ne laisse plus rien à désirer à cet égard. Car on ne peut chercher *séparément* aucune de ces racines, puisqu'elles jouissent de propriétés semblables, et qu'on ne peut concevoir aucune méthode qui conduise à l'une plutôt qu'à l'autre. Mais on les trouve toutes à la fois par cette opération arithmétique dont je viens de parler, et à peu près de la même manière qu'on obtiendrait tous les nombres inférieurs et premiers à un nombre donné. Or, il me semble qu'on n'a jamais trouvé qu'il y eût une difficulté particulière à déterminer actuellement ces derniers nombres. Quand on veut les avoir, on considère les facteurs simples du nombre donné; et de la suite naturelle 1, 2, 3, 4, 5, etc., on exclut tous les multiples de ces facteurs simples. Ici, au lieu de ces multiples, il faut exclure toutes les puissances d'exposants marqués par ces mêmes facteurs : c'est, comme on voit, une opération du même genre, mais d'un ordre plus élevé.

ARTICLE IV.

Sur l'ordre naturel dans lequel doivent être rangées les racines des équations binômes

18. Considérons l'équation

$$x^p - 1 = \mathfrak{M}\,P,$$

où l'exposant p est un diviseur de $P-1$, les nombres p et P étant tous deux premiers.

Soit r une quelconque des racines de cette équation, autre que l'unité; comme le nombre p est premier, r sera une racine primitive, et par conséquent toutes les racines pourront s'exprimer par

la suite

$$r,\ r^2,\ r^3,\ r^4,\ r^5,\ r^6,\ldots,\ r^{p-1}.$$

Mais cet ordre, qui nous paraît naturel, n'est pas le plus simple : on peut ranger ces $p-1$ racines de manière que chacune soit toujours une même puissance de celle qui la précède. Et, en effet, soit a une racine primitive de

$$x^{p-1} - 1 = \mathcal{M} p\,;$$

les $p-1$ exposants de r,

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ldots,\ p-1,$$

pourront se ranger dans l'ordre nouveau

$$a,\ a^2,\ a^3,\ a^4,\ a^5,\ a^6,\ldots,\ a^{p-1},$$

en négligeant les multiples de p, ce qui est permis, puisque r^p se réduit à 1. On aura donc, pour la représentation des $p-1$ racines de

$$x^p - 1 = \mathcal{M}\,\mathrm{P},$$

autres que l'unité, cette suite

$$r,\ r^a,\ r^{a^2},\ r^{a^3},\ r^{a^4},\ldots,\ r^{a^{p-2}},$$

qui est la plus simple et la plus naturelle de toutes, puisque toutes les racines y naissent l'une de l'autre par la même puissance : de sorte qu'elles sont exprimées à l'aide d'une seule quelconque d'entre elles et d'un seul et même signe d'opération.

Si vous changez la racine r en une autre quelconque de la suite

$$r,\ r^a,\ r^{a^2},\ r^{a^3},\ldots,$$

il est visible que vos racines se suivront toujours dans le même ordre qu'auparavant. Si vous changez l'exposant a en un autre b qui soit aussi une racine primitive de

$$x^{p-1} - 1 = \mathcal{M}\, p,$$

comme b ne sera autre chose que a élevée à quelque puissance e première à $p-1$, il est clair que l'ordre nouveau

$$r,\ r^b,\ r^{b^2},\ r^{b^3},\ r^{b^4},\ldots$$

ne sera autre chose que le premier où les racines seraient prises de e en e. Ainsi, soit qu'on change la racine r d'où l'on part, soit qu'on change l'exposant a à l'aide duquel on produit les racines l'une apres l'autre, la disposition mutuelle de ces racines n'en peut être troublée; elles demeurent toujours équi-distantes, comme si elles étaient rangées en cercle. C'est à cet ordre remarquable que tient la résolution algébrique des équations binômes, et, en général, celle de toute équation où l'inconnue est une fonction des racines de l'unité : ce qui comprend au fond, comme on peut le démontrer, toutes les équations possibles à racines périodiques (*voyez* le tome IV des *Mémoires de l'Académie des Sciences*).

19. On voit, par ce que je viens d'indiquer rapidement, combien la considération des racines primitives est importante, et que si l'on trouve une seule r de ces racines pour le nombre p, on pourra résoudre sur-le-champ toute équation binôme

$$x^n - A = \mathfrak{M}\, p.$$

Car cette équation n'est possible qu'autant que A est une puissance $n^{ième}$ exacte relativement à p; et par conséquent, il faudra qu'on ait

$$A = r^{in}.$$

Il n'y aura donc qu'à chercher dans la suite des puissances r^n, r^{2n}, r^{3n},... celle qui donne le résidu A; elle sera de la forme r^{in}, et l'équation

$$x^n - A = \mathfrak{M}\, p,$$

qui deviendra

$$x^n - r^{in} = \mathfrak{M}\, p,$$

donnera tout de suite

$$x = r^i;$$

et multipliant cette valeur r^i par les racines de

$$y^n - 1 = \mathfrak{M}\, p,$$

lesquelles seront au nombre de θ, si θ est le plus grand commun diviseur de n et $p - 1$, on trouvera les θ racines différentes de la proposée.

On peut tirer de là tous les théorèmes qui regardent la résolution des équations binômes

$$x^n - A = \mathfrak{M} p.$$

20. Au reste, on peut toujours abaisser immédiatement la proposée à une équation semblable du degré θ. Car, soient

$$n = n'\theta, \quad \text{et} \quad p - 1 = p'\theta,$$

n' et p' étant premiers entre eux : la proposée donne d'abord, en négligeant les multiples de p,

$$x^{n'\theta} - A = 0, \quad \text{ou} \quad x^{n'\theta} = A;$$

d'où, en extrayant la racine $n'^{ème}$ de part et d'autre, on tire

$$x^\theta = \sqrt[n']{A} = A^{\frac{1}{n'}}, \quad \text{ou bien} \quad x^\theta - A^{\frac{1}{n'}} = 0;$$

et il ne s'agit plus que de réduire l'exposant fractionnaire $\frac{1}{n'}$ à un entier φ, sans changer la valeur de l'exponentielle. Mais, par hypothèse, A étant une puissance exacte de degré $n = n'\theta$, est aussi, par là même, une puissance de degré θ; le nombre A est donc racine de l'équation

$$x^{\frac{p-1}{\theta}} - 1 = 0,$$

qui renferme toutes les puissances θ des différents nombres

$$1, 2, 3, 4, 5, 6, \ldots, p - 1;$$

et, par conséquent, on a

$$A^{\frac{p-1}{\theta}} = 1, \quad \text{ou} \quad A^{p'} = 1.$$

Donc, à tout exposant de A il est toujours permis d'ajouter un multiple arbitraire de p', et au lieu de A, on peut mettre $A^{1+\mathfrak{M}p'}$, $\mathfrak{M}$ étant un multiple quelconque. Mais si l'on veut actuellement tirer la racine $n'^{ème}$ de A, il faut choisir ce multiple $\mathfrak{M}$ de manière que l'exposant $1 + \mathfrak{M}p'$ soit exactement divisible par n'; ce qui donne l'équation du premier degré

$$1 + \mathfrak{M}p' = n'\varphi,$$

équation toujours possible, puisque les coefficients p' et n' sont premiers entre eux. Ainsi l'on trouvera toujours un entier φ équivalent à l'exposant fractionnaire $\frac{1}{n'}$, et l'on aura

$$\sqrt[n']{A}, \quad \text{ou} \quad A^{\frac{1}{n'}} = A^{\varphi},$$

et la proposée

$$x^n - A = \mathfrak{M}\, p$$

sera ramenée à la forme

$$x^{\theta} - A^{\varphi} = \mathfrak{M}\, p,$$

θ étant le plus grand commun diviseur de n et de $p-1$; *ce qu'il fallait trouver.*

Ainsi, quand on propose une équation binôme de la forme

$$x^n - A = \mathfrak{M}\, p,$$

on peut supposer qu'elle est déjà réduite, de manière que le degré n soit un diviseur de $p-1$; ce qui simplifie le calcul, sans rien ôter à la généralité de la question.

Mais cette méthode élégante qu'on vient de suivre pour abaisser l'équation au degré marqué par le plus grand commun diviseur de n et $p-1$, nous donne l'idée d'une méthode semblable par laquelle on pourrait essayer d'abaisser de même cette réduite au premier degré, et d'obtenir par là une solution directe de la proposée.

Article V.

Solution directe de l'équation $x^n - A = \mathfrak{M}\, p$.

21. Soit

$$x^n - A = \mathfrak{M}\, p,$$

ou plus simplement

$$x^n = A$$

(n étant supposé diviseur de $p-1$); j'en tire, comme ci-dessus,

$$x = \sqrt[n]{A} = A^{\frac{1}{n}};$$

et il ne s'agit plus que de réduire l'exposant $\frac{1}{n}$ à un entier e, sans changer la valeur de $A^{\frac{1}{n}}$. Or A étant une puissance $n^{\text{ième}}$ exacte, est par cela même une racine de

$$x^{\frac{p-1}{n}} - 1 = 0,$$

et l'on a

$$A^{\frac{p-1}{n}} = 1.$$

Ainsi à tout exposant de A il est permis d'ajouter un multiple quelconque de $\frac{p-1}{n}$, et l'on peut écrire, au lieu de A, $A^{1+\mathfrak{M}\frac{p-1}{n}}$. Pour en tirer la racine $n^{\text{ième}}$, il n'y a donc qu'à rendre ce nouvel exposant $1 + \mathfrak{M}\frac{p-1}{n}$ exactement divisible par n, ce qui donne l'équation indéterminée

$$1 + \mathfrak{M}\left(\frac{p-1}{n}\right) = ne.$$

Or, cette équation est possible lorsque n et $\frac{p-1}{n}$ sont premiers entre eux. Dans ce cas, on déterminera sur-le-champ l'exposant inconnu e qui équivaut à $\frac{1}{n}$, et l'on aura, pour une des racines de la proposée,

$$x = A^e.$$

Soient, par exemple,

$$p = 13, \quad n = 3,$$

et la proposée

$$x^3 - 8 = \mathfrak{M}(13);$$

on aura, pour une des racines,

$$x = 8^e,$$

l'exposant e étant donné par l'équation du premier degré

$$1 + \mathfrak{M}\,4 = 3e.$$

Cette équation est possible, puisque 3 et 4 sont premiers entre eux,

et elle donne, pour la valeur de e,

$$e = -1,$$

ou, si l'on veut,

$$e = 3,$$

d'où il vient

$$x = 8^3 = 5,$$

qui est effectivement une des racines cubiques de 8, relativement au nombre premier 13.

22. Voilà donc une méthode directe qui apprend à trouver une solution de l'équation binôme $x^n - A = \mathfrak{M}\, p$, lorsque le degré n (diviseur de $p-1$) est premier à $\frac{p-1}{n}$; ce qui fait deux fois autant de cas qu'il y a de manières de partager le nombre composé $p-1$ en deux facteurs premiers entre eux.

Mais il se présente ici une difficulté singulière qu'il est important de proposer et de résoudre, parce qu'elle touche aux points fondamentaux de la théorie.

Difficulté singulière sur la solution qui précède.

23. Quand on se propose de trouver les racines $n^{ièmes}$ du nombre A, que je suppose être une puissance $n^{ième}$ exacte, on ne conçoit pas d'abord qu'il puisse y avoir aucune méthode par laquelle on dégage une de ces racines, de préférence aux autres, puisque toutes sont également définies par la même équation ou la même propriété de donner

$$x^n = A.$$

Et pourtant, par la voie que j'ai suivie, je viens de trouver une de ces racines en particulier, et d'obtenir, à l'aide d'une équation du premier degré, un certain exposant entier e qui est tel qu'on a

$$A^e = x.$$

On pourrait croire d'abord que cette expression A^e renferme une certaine équivoque, et qu'elle est également propre à représenter les autres racines, en ajoutant, ce qui est permis, à l'exposant e différents multiples de $\frac{p-1}{n}$. Mais il est évident, à cause de $A^{\frac{p-1}{n}} = 1$, qu'on re

tomberait toujours sur la même valeur de x; de sorte qu'on a une expression A^e, délivrée de toute équivoque, et qui répond à une certaine racine choisie entre les n racines semblables de la proposée : ce qui mérite bien d'être expliqué.

Solution de la difficulté.

24. Pour résoudre cette difficulté, sans rompre la suite de notre raisonnement, nous devons donc faire voir tout de suite que, parmi les n racines de A, il n'y en a qu'une seule qui jouisse de la propriété de pouvoir être représentée par une puissance entière du nombre A : or, c'est ce qu'on peut démontrer par la nature même de la question.

Et, en effet, s'il est possible qu'une des racines $n^{ièmes}$ de A soit représentée par une puissance entière A^e du nombre A lui-même, comme, par hypothèse, A est une puissance exacte du degré n, A^e sera aussi une puissance exacte du même degré n. Donc A^e sera tout à la fois racine de la proposée

$$x^n - A = 0,$$

et racine de l'équation

$$x^{\frac{p-1}{n}} - 1 = 0.$$

Or il est aisé de voir que ces deux équations binômes ont une racine commune et qu'elles n'en peuvent avoir qu'une seule, précisément parce qu'elles sont de degrés n et $\frac{p-1}{n}$ premiers entre eux.

C'est ce qu'on peut prouver directement par la recherche actuelle du commun diviseur entre les deux binômes

$$x^n - A, \quad \text{et} \quad x^{\frac{p-1}{n}} - 1.$$

Car soit, pour abréger,

$$\frac{p-1}{n} = m;$$

et supposons qu'on ait :

$$\begin{aligned} m &= nq + r, \\ n &= rq' + r', \\ r &= r'q'' + r'', \\ r' &= r''q''' + r''', \\ &\dots\dots\dots \end{aligned}$$

(n étant $< m$, $r < n$, $r' < r$, $r'' < r'$,...).

Si l'on fait l'opération du commun diviseur entre les deux binômes $x^m - 1$ et $x^n - A$, jusqu'à ce que le plus petit exposant n soit tombé au-dessous de m, on aura d'abord le premier reste

$$A^q x^r - 1;$$

si l'on fait ensuite la même opération entre $x^n - A$ et ce reste $A^q x^r - 1$, on arrivera au deuxième reste

$$x^{r'} - A^{1+qq'};$$

si l'on fait la même opération entre

$$A^q x^r - 1 \quad \text{et} \quad x^{r'} - A^{1+qq'},$$

on arrivera au troisième reste

$$A^{q+q''(1+qq')} x^{r''} - 1;$$

et si l'on continuait, on trouverait pour le reste suivant

$$x^{r'''} - A^{1+qq'+q'''[q+q''(1+qq')]},$$

et ainsi de suite. D'où l'on voit que les exposants successifs de x sont les restes r, r', r'', r''',... de la division de m par n, de n par r, de r par r', etc.; et que les exposants de A sont les numérateurs successifs des fractions convergentes vers la fraction $\frac{m}{n}$ dans le développement de cette valeur en fraction continue.

Mais si m et n sont premiers entre eux, on arrive nécessairement à quelque reste tel que r'' qui est égal à l'unité; et le reste suivant r''' est égal à zéro.

Donc, par l'opération du commun diviseur entre les binômes proposés, on arrive nécessairement à un reste du premier degré, tel que

$$A^{q+q''(1+qq')} x - 1,$$

et le reste suivant est

$$x^0 - A^{1+qq'+q'''[q+q''(1+qq')]}.$$

Or ce reste est nul par hypothèse; car l'exposant de A est alors le numérateur même de la fraction proposée $\frac{m}{n}$, qui est la dernière des frac-

tions convergentes ; et par conséquent, le reste dont il s'agit se réduit à

$$x^0 - A^m \quad \text{ou} \quad 1 - A^m,$$

qui est nul par hypothèse.

Donc, les deux binômes proposés ont le commun diviseur du premier degré,

$$A^{q+q''(1+qq')}x - 1,$$

lequel, égalé à zéro, donne

$$x = A^{-q-q''(1+qq')}.$$

Cette expression s'accorde parfaitement avec l'expression A^e que nous avons trouvée ci-dessus d'une manière directe : car le nombre e était déterminé par l'équation

$$1 + \mathfrak{M}\, m = ne,$$

et cette équation, résolue par la méthode des fractions continues, donne

$$e = -q - q'' - qq'q'';$$

ce qui est, abstraction faite du signe, le numérateur de la fraction convergente qui précède immédiatement la fraction $\frac{m}{n}$. Quant au signe *moins*, il tient ici au quantième du terme où l'on a supposé que la fraction continue s'arrête : si elle avait un terme de moins, ou un terme de plus, on aurait trouvé l'exposant e positif. Au reste, quand on aura un exposant négatif $-e$, on pourra toujours le changer en un autre qui soit positif, en écrivant A^{m-e} au lieu de A^{-e}.

On voit donc que, si m et n sont premiers entre eux, les deux équations binômes

$$x^m - 1 = 0, \quad \text{et} \quad x^n - A = 0,$$

ont une racine commune, et n'en peuvent avoir qu'une seule; et que la première méthode qu'on a suivie ne pouvait conduire qu'à cette racine singulière de la proposée

$$x^n - A = 0,$$

racine distinguée des $n - 1$ autres en ce que cette valeur est à la

fois une racine $n^{ième}$ de A, et une puissance $n^{ième}$ de quelque autre nombre.

25. Au reste, on aurait encore pu arriver au résultat précédent par une opération plus simple sur les deux équations proposées

$$x^m = 1 \quad \text{et} \quad x^n = A.$$

Car, à cause de $m = nq + r$, la première devient

$$x^{nq}.x^r = 1,$$

et mettant pour x^n sa valeur A tirée de la seconde, on trouve d'abord

$$A^q x^r = 1, \quad \text{ou} \quad x^r = A^{-q};$$

mais, de même, à cause de $n = rq' + r'$, $x^n = A$ devient

$$x^{rq}.x^{r'} = A,$$

et mettant pour x^r sa valeur A^{-q}, on trouve

$$A^{-qq'}.x^{r'} = A, \quad \text{ou bien} \quad x^{r'} = A^{1+qq'};$$

de la même manière, on trouverait

$$x^{r''} = A^{-q-q''(1+qq')},$$

etc., etc., comme ci-dessus.

Si l'on suppose de même $r'' = 1$, et partant, $r''' = 0$, on arrive également à l'équation

$$x = A^{-q-q''(1+qq')},$$

qui est vraie pourvu qu'on ait aussi la suivante

$$x^0 - A^m, \quad \text{ou} \quad 1 - A^m = 0,$$

ce qui est la condition qui a lieu ici par hypothèse.

26. Quand les exposants m et n ne sont pas premiers entre eux, l'équation

$$1 + \mathfrak{M} = ne$$

est impossible, et si m est la plus petite puissance de A qui amène l'unité; c'est-à-dire si le nombre A est une des *racines primitives* de

$$A^m - 1 = 0,$$

on peut conclure qu'il n'y a aucune expression de la forme A^e qui puisse être racine de la proposée

$$x^n - A = o.$$

Mais si A, qui satisfait toujours à l'équation

$$A^m - 1 = o,$$

n'est simplement *racine primitive* que d'une équation inférieure

$$A^{m'} - 1 = o,$$

et que m' soit premier à n, la proposée aura encore une racine de la forme A^e. Car on trouverait, comme précédemment,

$$x = \sqrt[n]{A} = A^{\frac{1}{n}},$$

ou, à cause de $A^{m'} = 1$,

$$x = A^{\frac{1 + \mathfrak{M}\, m'}{n}} = A^e,$$

l'exposant e étant donné par l'équation

$$1 + \mathfrak{M}\, m' = ne,$$

qui est possible, quand on suppose m' et n premiers entre eux

Si cette dernière condition n'a pas lieu, la proposée ne peut avoir encore de racine de la forme A^e.

27. Nous voyons donc que *l'équation*

$$x^n - A = \mathfrak{M}\, p$$

ne peut jamais avoir de racine de la forme A^e : 1° *Quand* A *est une des racines primitives de l'équation*

$$A^{\frac{p-1}{n}} - 1 = \mathfrak{M}\, p;$$

2° *Quand* A *est racine primitive de quelque autre équation de degré* m' *qui n'est pas premier avec* n.

Ces deux cas enveloppent tous les autres; car, quel que soit le nombre donné A, il est nécessairement racine primitive, ou de

$$A^m - 1 = \mathfrak{M}\, p,$$

ou de quelque autre équation inférieure de degré m' diviseur de m.



Dans l'application, pour découvrir ce degré m', ou cette équation

$$A^{m'} - 1 = \mathfrak{M}\, p,$$

dont A est racine primitive, il n'y aura rien de plus simple que de faire les puissances successives de A, jusqu'à ce qu'on en trouve une $A^{m'}$ qui donne l'unité. On déterminera ensuite le plus grand commun diviseur θ de m' et n. Si l'on a $\theta > 1$, il n'y aura aucune racine de la forme A^e à chercher. Si l'on a $\theta = 1$, il y en aura une $x = A^e$, et l'exposant e sera donné par l'équation du premier degré

$$1 + \mathfrak{M}\, m' = ne.$$

28. Mais je n'étendrai pas plus loin la recherche et l'examen de ces méthodes directes qu'on pourrait imaginer pour la résolution des équations binômes

$$x^n - A = \mathfrak{M}\, p.$$

Ce qu'il y a de plus simple et de plus général est de chercher d'abord une racine primitive r de l'équation

$$x^{p-1} - 1 = \mathfrak{M}\, p.$$

On formera sur-le-champ la suite des puissances

$$r,\ r^2,\ r^3,\ r^4,\ r^5,\ r^6,\ r^7,\ldots,\ r^{p-1},$$

et l'on écrira au-dessous les différents nombres qu'elles donnent relativement à p, et qui composent tous les nombres inférieurs $1, 2, 3, \ldots, p-1$. Au moyen de ce tableau, on résoudra à la première vue toutes les équations binômes qui se rapporteraient au module p, et l'on exécutera avec la plus grande facilité toutes les opérations qu'on pourrait avoir à faire sur les racines.

Article VI.

De l'équation binôme $x^n - 1 = \mathfrak{M}\, p^m$, où le module est une puissance quelconque p^m d'un nombre premier p supérieur à 2.

29. Soit n le nombre $p^{m-1}(p-1)$ qui marque combien il y a de nombres $1, e, e', e'', \ldots$, inférieurs et premiers à p^m; l'équation

$$x^n - 1 = \mathfrak{M}\, p^m$$

aura, comme on sait, les n racines entières $1, e, e', e'', \ldots$, et n'en aura pas davantage au-dessous du module p^m.

30 Maintenant je dis que *l'équation*

$$x^D - 1 = \mathfrak{M} p^m,$$

où D *est un diviseur quelconque de n, ne peut avoir plus de* D *racines différentes au-dessous de* p^m.

Ce diviseur D de n, c'est-à-dire de $p^{m-1}(p-1)$, ne peut être que de la forme θp^ν ; θ étant un diviseur de $p-1$, et ν un exposant quelconque $< m$: il s'agit donc de démontrer que l'équation

$$x^{\theta p^\nu} - 1 = \mathfrak{M} p^m$$

ne peut avoir plus de θp^ν racines différentes inférieures à p^m.

Comme cette démonstration est longue et difficile, j'aurai soin de la diviser, et d'en ordonner les parties de manière à y ménager comme autant de points de repos.

Démonstration.

I. Je remarque d'abord que, quelles que soient les racines de cette équation, relative au module p^m, elles doivent satisfaire, à plus forte raison, à la même équation rapportée au simple module p, c'est-à-dire à l'équation $x^{\theta p^\nu} - 1 = \mathfrak{M} p$. Mais il est clair que toutes les racines de celle-ci doivent satisfaire à l'équation $x^\theta - 1 = \mathfrak{M} p$, puisque θ est le plus grand commun diviseur de θp^ν et $p-1$. Donc toutes les racines de la proposée doivent satisfaire à la simple équation

$$x^\theta - 1 = \mathfrak{M} p.$$

Or celle-ci ne peut avoir que θ racines différentes $a, b, c, \ldots$ en nombres inférieurs à p; et, par conséquent, tous les nombres possibles qui peuvent y satisfaire sont nécessairement de la forme

$$a + \mathfrak{M} p, \quad b + \mathfrak{M} p, \quad c + \mathfrak{M} p, \ldots;$$

donc toutes les racines de la proposée doivent se rapporter aux θ formes différentes

$$a + \mathfrak{M} p, \quad b + \mathfrak{M} p, \quad c + \mathfrak{M} p, \ldots.$$

II. Soit donc α une de ces racines qui répondent à la forme $a + \mathfrak{M} p$. Si l'on prouvait, en premier lieu, que $\alpha + yp^{m-\nu}$ en est une autre, quel que soit y, il s'ensuivrait qu'on en peut compter ainsi un nombre p^ν, en donnant à y les p^ν valeurs successives 0, 1, 2, 3, 4,... jusqu'à $p^\nu - 1$; et sans aller au delà, puisque les racines $\alpha + yp^{m-\nu}$ reviendraient alors aux précédentes, mais prises au-dessus du module p^m.

Si l'on prouvait, en second lieu, que toute autre racine α' qui répondrait à la même forme que α, c'est-à-dire à la forme $\alpha + \mathfrak{M} p$, et d'où résulterait ainsi

$$\alpha' = \alpha + \mathfrak{M} p,$$

retombe nécessairement sur une de celles que je viens d'énumérer, il s'ensuivrait que la proposée ne peut avoir plus de p^ν racines différentes relatives à a, plus de p^ν racines relatives à b, etc., et, par conséquent, plus de θp^ν racines différentes, au-dessous du module p^m.

III. Pour établir le premier des deux points qu'on vient de supposer, il suffirait de prouver que si l'on cherche, par le binôme de Newton, le développement de $(\alpha + yp^i)^{\theta p^\nu}$, on trouvera un résultat de cette forme

$$(\alpha + yp^i)^{\theta p^\nu} = \alpha^{\theta p^\nu} + \mathrm{Y} p^{i+\nu},$$

où Y est un entier. Car, en faisant $i + \nu = m$, c'est-à-dire $i = m - \nu$, on verrait que le second membre se réduit à $1 + \mathfrak{M} p^m$, puisque α étant racine par hypothèse, $\alpha^{\theta p^\nu}$ se réduit à $1 + \mathfrak{M} p^m$: d'où l'on pourrait conclure que si α est racine de la proposée, $\alpha + yp^{m-\nu}$ en est une autre quel que soit y: ce qui est la première de nos deux suppositions.

Ensuite, il faudrait prouver que, si y est premier à p, le multiple Y est aussi premier à p: de sorte que $p^{i+\nu}$ est la plus haute puissance de p, par laquelle on puisse diviser le terme $\mathrm{Y} p^{i+\nu}$, et qu'ainsi $\alpha + yp^i$ ne peut être racine si l'exposant i tombe au-dessous de $m - \nu$. Car il s'ensuivra que toute racine α' relative au résidu a, et par conséquent de la forme $\alpha + yp^i$, retombe nécessairement dans la forme $\alpha + yp^{m-\nu}$: ce qui est la seconde de nos deux suppositions.

IV. Tout se réduit donc enfin à démontrer que l'on a toujours, quel que soit y, l'équation

$$(\alpha + yp^i)^{\theta p^\nu} = \alpha^{\theta p^\nu} + \mathrm{Y} p^{i+\nu},$$

telle, que Y est un nombre entier; et que, si y est premier à p, le nombre Y est aussi premier à p.

V. La démonstration immédiate de ce théorème, qui paraît facile au premier coup d'œil, présente néanmoins beaucoup de difficultés, à cause de l'exposant composé θp^ν d'où naissent les coefficients du binôme. Mais voici un moyen très-simple de sortir de cet embarras, et d'arriver au théorème de la manière la plus claire et la plus rapide. C'est de supposer qu'au lieu d'élever tout d'un coup le binôme $\alpha + yp^i$ à la puissance θp^ν, on l'élève d'abord à la simple puissance p; et puis le résultat obtenu à la puissance p; et ainsi de suite, jusqu'à ce qu'on arrive au résultat qui réponde à la puissance p^ν; et enfin, de supposer qu'on forme la puissance θ de ce dernier résultat.

Or, en élevant le binôme $\alpha + yp^i$ à la puissance p, on a

$$(\alpha + yp^i)^p = \alpha^p + p.\alpha^{p-1}yp^i + \frac{p.\overline{p-1}}{2}\alpha^{p-2}y^2p^{2i} + \ldots,$$

où l'on voit que le second terme est divisible par p^{i+1}, et que tous les autres le sont, au moins par p^{i+2}, pourvu que le nombre premier p soit > 2 : car le coefficient du troisième terme, qui est $\frac{p.\overline{p-1}}{2}$, est alors divisible par p, et par conséquent ce troisième terme est divisible par p^{2i+1}, et l'est ainsi, au moins, par p^{i+2}, puisque i est supposé être au moins 1 : quant aux autres termes qui contiennent p^{3i}, p^{4i}, etc., il est évident qu'ils sont au moins divisibles par p^{i+2}; on a donc

$$(\alpha + yp^i)^p = \alpha^p + \mathrm{Y}_{,}p^{i+1},$$

où $\mathrm{Y}_{,}$ est un nombre entier. Et l'on voit, de plus, que cet entier $\mathrm{Y}_{,}$ est de la forme $\alpha^{p-1}y + \mathfrak{M}p$: si donc y est premier à p (comme α l'est aussi par hypothèse), le multiple $\mathrm{Y}_{,}$ sera aussi premier à p.

Mais par la même raison, en élevant le nouveau binôme $\alpha^p + \mathrm{Y}_{,}p^{i+1}$ à la puissance p, ce qui donnera la puissance p^2 du premier binôme $\alpha + yp^i$, on trouvera

$$(\alpha + yp^i)^{p^2} = \alpha^{p^2} + \mathrm{Y}_{,,}p^{i+2},$$

où $\mathrm{Y}_{,,}$ sera un entier, premier à p, si $\mathrm{Y}_{,}$, et par conséquent si y est pre-

mier à p. Et ainsi de suite; d'où l'on conclut

$$(\alpha + yp^{t})^{p^{\nu}} = \alpha^{p^{\nu}} + Y_{\nu}p^{t+\nu},$$

où Y_{ν} est un entier, premier à p si y est premier à p.

Actuellement, qu'on élève à la puissance θ, et il vient

$$(\alpha + yp^{t})^{\theta p^{\nu}} = \alpha^{\theta p^{\nu}} + Yp^{t+\nu},$$

où il est évident que Y est un entier de la forme

$$\theta.\alpha^{p^{\nu}(\theta-1)}.Y_{\nu} + \mathfrak{M}\,p;$$

or, si y est premier à p, comme Y_{ν} le sera aussi, et que α et $\theta < p$ le sont aussi par hypothèse, il s'ensuit que Y sera aussi premier à p. Ce qui donne enfin *le théorème général qu'il s'agissait de démontrer.*

31. Il résulte de là que l'équation

$$x^{n} - 1 = \mathfrak{M}\,p^{m},$$

où le nombre n est égal à $p^{m-1}(p-1)$, a des *racines primitives,* c'est-à-dire des racines qui, par leurs puissances successives 0, 1, 2, 3,..., $n-1$, sont propres à former la série complète de tous les nombres 1, e, e', e'',... inférieurs et premiers à p^{m}. Car, puisque aucune équation

$$x^{D} - 1 = \mathfrak{M}\,p^{m},$$

où D est diviseur de n, ne peut avoir plus de D racines différentes au-dessous de p^{m}, on démontrera ici, par un raisonnement tout à fait semblable à celui du n° **12**, que parmi les n racines de la proposée, il y en a au moins une qui, par ses puissances successives 0, 1, 2, 3,..., $n-1$, ne ramènera point l'unité avant la puissance $n^{\text{ième}}$, et qui, par conséquent, formera la suite complète de toutes les racines de la proposée.

Et maintenant, si r est une de ces racines primitives, il est clair que toute puissance r^{h}, d'exposant h premier à n, en est une autre; et que toute puissance r^{q}, d'exposant q diviseur de n, est une racine primitive de l'équation binôme inférieure

$$x^{\frac{n}{q}} - 1 = \mathfrak{M}\,p^{m}.$$

12..

32. Enfin, tout ce qu'on vient de démontrer pour un module p^m qui est une puissance d'un nombre premier supérieur à 2, peut également s'appliquer au cas où le module est le double de cette puissance, c'est-à-dire est égal à $2p^m$.

En effet, en considérant l'équation

$$x^n - 1 = \mathfrak{M}(2p^m),$$

où le nombre n qui marque combien il y a de nombres inférieurs et premiers à $2p^m$ est le même que ci-dessus, c'est-à-dire est $p^{m-1}(p-1)$, on ferait voir de la même manière que l'équation

$$x^{\theta p^\nu} - 1 = \mathfrak{M}(2p^m)$$

ne peut avoir que θp^ν racines différentes au-dessous de $2p^m$. Car ces racines devant toutes satisfaire à la simple équation

$$x^\theta - 1 = \mathfrak{M}(2p),$$

et celle-ci ne pouvant avoir plus de θ racines en nombres $a, b, c,\ldots$ inférieurs à $2p$, il s'ensuit que toutes les racines de la proposée doivent entrer dans les θ formes

$$a + \mathfrak{M}\,p, \quad b + \mathfrak{M}\,p, \quad c + \mathfrak{M}\,p, \ldots,$$

et que, par conséquent, si α est une racine de la forme $a + \mathfrak{M}\,p$, où a est nécessairement *impair* et $\mathfrak{M}$ *pair*, $\alpha + yp^{m-\nu}$ en est une autre, quel que soit le multiple pair y, pris depuis 0 jusqu'à $2p^\nu - 2$, ce qui fait en tout p^ν valeurs différentes au-dessous de $2p^m$.

On ferait voir que toute autre racine α' se rapportant à la même forme $a + \mathfrak{M}\,p$, rentrerait nécessairement dans les précédentes, etc.; d'où résulte exactement, pour les équations binômes rapportées au double d'une puissance d'un nombre premier, la même suite de propriétés que pour les équations binômes rapportées à la simple puissance de ce nombre premier.

33. Quand le nombre premier p est égal à 2, toutes ces propriétés n'ont plus lieu; et l'équation

$$x^n - 1 = \mathfrak{M}\,2^m$$

ne peut plus avoir de racines primitives, excepté dans le cas unique

de $m = 2$, ce qui donne le module 2^m égal à 4. En effet, l'exposant n, qui devient alors égal à 2, ne peut avoir au-dessous de lui d'autre diviseur que l'unité; or, l'équation

$$x - 1 = \mathfrak{M}(2^2)$$

ne pouvant avoir qu'une seule racine 1, il s'ensuit que la proposée

$$x^2 - 1 = \mathfrak{M}(2^2),$$

qui a deux racines, en a nécessairement une qui est *primitive*.

Au reste, la raison de cette exception particulière se trouve encore dans la propriété qu'ont les équations binômes rapportées au double d'un simple nombre premier p, d'avoir des racines primitives, *quel que soit* p, et par conséquent dans le cas même où $p = 2$.

Manière de résoudre l'équation $x^D - 1 = \mathfrak{M}\, p^m$ par l'équation $x^D - 1 = \mathfrak{M}\, p$.

34. Il résulte du théorème précédent que si α est une racine de

$$x^D - 1 = \mathfrak{M}\, p^m, \quad \text{où} \quad D = \theta p^\nu,$$

$\alpha + y p^{m-\nu}$ non-seulement en sera une autre, quel que soit y, mais encore sera une racine relative au module p^{m+1} si l'on choisit y d'une manière convenable.

En effet, on aura

$$(\alpha + y p^{m-\nu})^D = \alpha^D + \theta\alpha^{D-1}.y.p^m + \text{etc.},$$

où le reste des termes marqué par etc. est au moins divisible par p^{m+1}; or, puisqu'on a, par hypothèse,

$$\alpha^D - 1 = Ap^m,$$

il viendra

$$(\alpha + y p^{m-\nu})^D = 1 + (A + \theta\alpha^{D-1}.y)\, p^m + \text{etc.};$$

donc si l'on choisit y de manière à rendre le coefficient $(A + \theta\alpha^{D-1}.y)$ divisible par p, tout le reste des termes après le premier 1, sera divisible par p^{m+1}; il n'y a donc qu'à déterminer y par l'équation du premier degré

$$A + \theta.\alpha^{D-1}.y = \mathfrak{M}\, p,$$

équation toujours possible; car le coefficient de y est premier à p, et A est aussi premier à p, puisque α est supposé racine de

$$x^{\mathrm{D}} - 1 = \mathfrak{M}\, p^m,$$

pour le module p^m, et non pas pour le module plus élevé p^{m+1}.

Ainsi, quand on connaît une racine α qui appartient à l'équation

$$x^{\mathrm{D}} - 1 = \mathfrak{M}\, p^m,$$

et seulement pour le module p^m, de manière que le multiple $\mathfrak{M}$ est un nombre A qui n'est point divisible par p, on peut toujours trouver une racine $\alpha + yp^{m+1}$ qui résout la même équation pour le module plus élevé p^{m+1}; c'est-à-dire qu'on peut résoudre l'équation

$$x^{\mathrm{D}} - 1 = \mathfrak{M}\,(p^{m+1}).$$

Donc, si l'on a une racine de la proposée pour le simple module p, on en peut déduire une autre pour le module p^2, et de celle-ci une autre pour le module p^3, et ainsi de suite; de sorte que la résolution d'une equation

$$x^{\mathrm{D}} - 1 = \mathfrak{M}\, p^m$$

ne dépend que de la résolution de l'équation

$$x^{\mathrm{D}} - 1 = \mathfrak{M}\, p,$$

rapportée au simple module p.

ARTICLE VII.

De l'équation binôme $x^n - 1 = \mathfrak{M}\,(2^m)$, où l'exposant m du module 2^m est supérieur à 2.

35. Cette équation du degré $n = 2^{m-1}$ a toujours 2^{m-1} racines différentes $1, 3, 5, 7, 9, \ldots, 2^m - 1$, en nombres inférieurs et premiers au module 2^m; mais l'équation du degré sous-double 2^{m-2},

$$x^{2^{m-2}} - 1 = \mathfrak{M}\,(2^m),$$

a encore les mêmes racines : car ces racines étant nécessairement de la forme $1 + y.2$, il est facile de voir (en faisant le carré de ce binôme, et

puis le carré du résultat, et ainsi de suite), qu'on a toujours

$$(1 + y.2)^{2^\nu} = 1 + \mathfrak{M}\, 2^{\nu+2},$$

quel que soit y ; on a donc

$$(1 + y.2)^{2^{m-2}} = 1 + \mathfrak{M}\, 2^m.$$

Et cela peut se voir encore en observant que les racines peuvent toutes se mettre sous la forme $\pm\ 1 + y.2^2$; ce qui donne évidemment

$$(\pm\ 1 + y.2^2)^{2^{m-2}} = 1 + \mathfrak{M}\,(2^m).$$

Il résulte donc de là qu'aucune racine de la proposée ne peut, par ses puissances successives 0, 1, 2, 3,..., fournir plus de la moitié des nombres inférieurs et premiers à 2^m, et par conséquent ne peut être une racine primitive de l'équation

$$x^{2^{m-1}} - 1 = \mathfrak{M}\,(2^m).$$

36. Mais s'il n'y a point ici de racines primitives *absolues*, on peut démontrer, du moins, qu'il y a toujours quelque racine propre à fournir, par ses puissances, la *moitié* des 2^{m-1} résidus inférieurs et premiers à 2^m, ce qui mérite d'être remarqué.

En effet, si l'on considère le binôme $1 + y.2^i$, où je suppose que y soit impair, et i au moins égal à 2, il est facile de voir qu'on aura toujours l'équation

$$(1 + y.2^i)^{2^\nu} = 1 + \mathrm{Y}.2^{i+\nu},$$

où Y sera un entier impair.

Donc la plus haute puissance de 2, qui puisse diviser $(1 + y.2^i)^{2^\nu} - 1$, est $2^{i+\nu}$; donc pour que le binôme $1 + y.2^i$, élevé aux puissances successives 0, 2, 2^2, 2^3,..., puisse ramener l'unité par rapport au module 2^m, il faut au moins aller jusqu'à la puissance 2^ν, telle que $\nu + i$ soit égal à m.

Donc, si l'on donne à i la plus petite valeur qu'il puisse avoir dans le théorème précédent, et qui est $i = 2$, on aura le binôme $1 + y.2^2$, dont aucune puissance 2, 2^2, 2^3,... ne donnera l'unité avant la puissance 2^{m-2}. On ne pourra donc trouver 1 pour aucun des exposants 2, 4, 8,... qui forment tous les diviseurs de 2^{m-2} ; et comme, d'un autre côté, cela

ne pourrait avoir lieu pour aucun autre exposant sans avoir lieu pour son commun diviseur avec 2^{m-2}, il s'ensuit qu'on ne pourra trouver l'unité pour aucun des exposants 1, 2, 3, 4, 5,... inférieurs à 2^{m-2}.

Donc la racine $x = 1 + y.2^2$, où y est un impair, est une espèce de racine primitive de l'équation proposée, en ce qu'elle fournit par ses puissances successives 0, 1, 2, 3, 4, 5,... une moitié des 2^{m-1} racines différentes de cette proposée.

Et maintenant, il est clair qu'en prenant dans cette période de résidus le troisième terme, le cinquième, le septième, etc., on aura autant de ces sortes de racines primitives qu'il y a de nombres inférieurs et premiers au nombre 2^{m-2}, et que, par conséquent, il y en aura 2^{m-3}; c'est ce qui s'accorde d'ailleurs avec l'expression $1 + y.2^2$ de ces racines primitives, puisqu'on ne peut donner à y que les 2^{m-3} valeurs impaires 1, 3, 5, 7,..., $(2^{m-2} - 1)$.

Si, au lieu du binôme $1 + y.2^2$, on eût considéré le binôme $-1 + y.2^2$, on aurait trouvé exactement les mêmes propriétés; d'où je conclus, en donnant à y les mêmes valeurs que ci-dessus, qu'il y a encore 2^{m-3} nouvelles racines primitives de la même espèce que les précédentes.

37. Mais il faut bien remarquer que chacune de ces nouvelles racines fournit, par ses puissances, une moitié des résidus qui n'est pas la même que la moitié précédente, et que ces deux périodes n'auront de commun qu'une moitié de leurs termes, et, par conséquent, un quart de tous les résidus.

Ainsi, pour le cas de $m = 5$, ou pour le module $2^5 = 32$, on a l'équation

$$x^{16} - 1 = \mathfrak{M}(32),$$

qui a les seize racines 1, 3, 5, 7, 9,..., 31, et qui n'en a pas davantage au-dessous de 32. Mais l'équation

$$x^8 - 1 = \mathfrak{M}(32),$$

du degré sous-double, a les mêmes seize racines, de sorte que cette équation a deux fois plus de racines que d'unités dans l'exposant de son degré. Aucune des seize racines de la proposée ne pouvant donc passer la huitième puissance sans ramener l'unité, ne peut fournir plus de huit résidus différents par rapport au module 32; et il n'y a point de racines primitives absolues.

Mais il y en a, du moins, de relatives à la moitié des seize résidus dont il s'agit; et ces racines sont

$$1+4,\quad 1+3.4,\quad 1+5.4,\quad 1+7.4,\quad \text{ou bien}\quad 5,\ 13,\ 21,\ 29.$$

Et, par exemple, la première 5, étant élevée aux puissances successives 0, 1, 2, 3, 4, 5,.., fournit les huit racines différentes

$$1,\ 5,\ 25,\ 29,\ 17,\ 21,\ 9,\ 13;$$

et chacune des trois autres 13, 21, 29 fournirait exactement, mais dans un autre ordre, la même période de ces huit résidus.

Ensuite, il y en a quatre autres, savoir:

$$-1+4,\quad -1+3.4,\quad -1+5.4,\quad -1+7.4,\quad \text{ou bien}\quad 3,\ 11,\ 19,\ 27,$$

telles que chacune fournit aussi huit résidus différents

$$1,\ 3,\ 9,\ 27,\ 17,\ 19,\ 25,\ 11;$$

nouvelle période qui n'a de commun avec la première que les quatre termes 1, 9, 17, 25.

Ainsi, dans le polygone régulier de trente-deux côtés, si l'on joint les sommets de 5 en 5, et puis dans le nouveau polygone qui en résulte, si l'on joint encore les sommets de 5 en 5, et qu'on fasse de même dans le polygone résultant, et ainsi de suite, on produira dans un certain ordre huit des seize polygones réguliers différents de trente-deux côtés.

Et, en prenant un quelconque de ceux qui restent et faisant la même opération, on produira dans un ordre semblable les huit autres polygones réguliers; de sorte que les seize polygones réguliers de trente-deux côtés seront partagés en deux groupes semblables, où chaque polygone dérive du précédent par la même loi.

Mais cette manière de les partager en deux groupes n'est pas unique, car en employant une racine de la forme $-1+4y$, telle que la racine 3, on formera huit polygones réguliers qui ne seront pas les mêmes que les huit premiers dus à la racine 5 : il n'y en aura que quatre de communs aux deux périodes.

58. En général, la racine $x=1+y.2^i$, où y est impair, et i au moins

égal à 2, conduira à une période de 2^{m-i} racines différentes; et $x' = -1 + y.2^i$ conduira à une période d'autant de racines; mais ces deux périodes n'auront de commun que la moitié de leurs termes : car il est aisé de voir que les puissances paires de x' sont les seules qui puissent revenir, et qui reviennent en effet (dans un autre ordre, ce qui est indifférent) aux puissances paires de x.

39. Quant à la résolution de l'équation binôme

$$x^{2^{m-i}} - 1 = \mathfrak{M}\, 2^m,$$

elle n'a aucune difficulté, et il est évident que la forme de ses racines est

$$x = \pm 1 + y.2^i,$$

ce qui donne, en faisant

$$y = 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ldots,\ (2^{m-i} - 1),$$

2^{m-i+1} racines; c'est-à-dire deux fois plus qu'il n'y a d'unités dans l'exposant 2^{m-i} du degré de l'équation proposée.

Et il n'y a pas d'autres racines, puisque ces racines X seraient nécessairement de la forme $(\pm 1 + y.2^{i'})$, l'exposant i' étant $< i$, et y impair, et qu'alors la puissance 2^{m-i} de cette expression serait

$$1 + \mathrm{Y}.2^{i'+m-i},$$

Y étant impair; de sorte que $\mathrm{X}^{2^{m-i}} - 1$ serait tout au plus divisible par $2^{i'+m-i}$ moindre que le module 2^m.

40. Ainsi, pour le module 32, l'équation

$$x^8 - 1 = \mathfrak{M}\, 32$$

a seize racines $x = \pm 1 + y.2^2$, en faisant $y = 0, 1, 2, 3, 4, 5, 6, 7$.

L'équation

$$x^4 - 1 = \mathfrak{M}\, 32$$

en a huit de la forme $\pm 1 + y.2^3$ qu'on trouve en faisant $y = 0, 1, 2, 3$.

Enfin l'équation

$$x^2 - 1 = \mathfrak{M}\, 32$$

en a quatre de la forme $\pm 1 + y.2^4$, en y faisant $y = 0,\ 1$.

Il n'y a que l'équation simple

$$x - 1 = \mathfrak{M}\, 2^m,$$

et l'équation

$$x^{2^{m-1}} - 1 = \mathfrak{M}\, 2^m,$$

qui aient précisément autant de racines qu'il y a d'unités dans l'exposant de leur degré; toutes les autres en ont le double.

Mais en voilà assez sur le cas singulier du module égal à une puissance de 2; il faut voir maintenant ce qui regarde les équations binômes rapportées à des modules composés.

Article VIII.

De l'équation binôme $x^n - 1 = \mathfrak{M}(\mathrm{N})$, rapportée à un module composé N.

41. Soit $\mathrm{N} = \mathrm{A}^a.\mathrm{B}^b.\mathrm{C}^c\ldots$; A, B, C,... étant des nombres premiers absolument; si n est le nombre qui marque combien il y a de nombres $1, e, e', e'',\ldots$ inférieurs et premiers à N, on aura l'équation

$$x^n - 1 = \mathfrak{M}(\mathrm{N}),$$

qui admettra n racines $1, e, e', e'',\ldots$ et qui n'en aura pas davantage.

Mais x étant premier à N, est aussi premier à chacun des facteurs $\mathrm{A}^a, \mathrm{B}^b, \mathrm{C}^c,\ldots$ de ce nombre composé N; on aura donc aussi

$$x^\alpha - 1 = \mathfrak{M}(\mathrm{A}^a), \quad x^\beta - 1 = \mathfrak{M}(\mathrm{B}^b), \quad x^\gamma - 1 = \mathfrak{M}(\mathrm{C}^c),\ldots,$$

$\alpha, \beta, \gamma,\ldots$ étant les nombres qui marquent combien il y a de nombres inférieurs et premiers aux facteurs respectifs $\mathrm{A}^a, \mathrm{B}^b, \mathrm{C}^c,\ldots$. Or, soit m le plus petit nombre divisible à la fois par $\alpha, \beta, \gamma,\ldots$; il résulte des équations précédentes qu'on aura aussi

$$x^m - 1 = \mathfrak{M}(\mathrm{A}^a), \quad x^m - 1 = \mathfrak{M}(\mathrm{B}^b), \quad x^m - 1 + \mathfrak{M}(\mathrm{C}^c),\ldots,$$

c'est-à-dire que le binôme $x^m - 1$ sera divisible à la fois par les facteurs $\mathrm{A}^a, \mathrm{B}^b, \mathrm{C}^c,\ldots$ et par conséquent divisible par leur produit N, puisque ces facteurs sont premiers entre eux. On aura donc, pour une valeur quelconque de x,

$$x^m - 1 = \mathfrak{M}(\mathrm{N})$$

Mais le plus petit nombre m qui soit divisible à la fois par α, β, γ,... est toujours moindre que le produit $\alpha\beta\gamma$..., si ces nombres ne sont pas premiers entre eux ; or, excepté le cas où N serait simplement une puissance A^a d'un nombre premier A, ou le double de cette puissance, les nombres

$$\alpha = A^{a-1}(A-1), \quad \beta = B^{b-1}(B-1), \quad \gamma = C^{c-1}(C-1), \ldots$$

ne sont jamais premiers entre eux, puisqu'ils ont au moins le commun diviseur 2 ; on a donc nécessairement le nombre $m < n$.

Donc un nombre quelconque x, premier à N, étant élevé aux puissances successives 1, 2, 3, 4,..., amènera toujours l'unité pour résidu, avant qu'on arrive à la puissance n ; donc il n'y a pas de nombres x dont les puissances successives x, x^2, x^3, x^4,... puissent former tous les nombres inférieurs et premiers à N ; et par conséquent le nombre composé N, ou, pour mieux dire, l'équation

$$x^n - 1 = \mathfrak{M}(N),$$

ne peut avoir ce qu'on appelle des *racines primitives*.

42. Quand le nombre N est une puissance A^a d'un nombre premier, ou le double $2A^a$ de cette puissance, cette conclusion n'a plus lieu : car on a alors

$$n = A^{a-1}(A-1) = \alpha,$$

et le plus petit nombre m divisible par α est α lui-même ; ainsi l'on a

$$m = n,$$

et il n'est plus prouvé que, dans ce cas, l'équation

$$x^n - 1 = \mathfrak{M}(N)$$

ne puisse avoir des racines primitives : et, en effet, on a démontré ci-dessus que cette équation a toujours de telles racines.

43. Quant à la résolution de l'équation

$$x^n - 1 = \mathfrak{M}\, N$$

(où N est de la forme $A^a B^b C^c$...), ou, en général, de l'équation

$$x^n - 1 = \mathfrak{M}\, N,$$

dont le degré D est un diviseur de

$$A^{a-1}.B^{b-1}.C^{c-1}\ldots(A-1)(B-1)(C-1)\ldots,$$

elle n'offre pas non plus de difficulté, d'après ce qui a été dit précédemment sur la résolution des équations binômes rapportées à un module de la forme A^a : car chaque racine de la proposée doit satisfaire aux équations simples

$$x^D - 1 = \mathfrak{M}A^a,\quad x^D - 1 = \mathfrak{M}\,B^b,\quad x^D - 1 = \mathfrak{M}\,C^c,\ldots.$$

Soient donc λ les racines de la première, μ celles de la seconde, ν celles de la troisième, etc.; chaque racine x de la proposée est donc à la fois des formes suivantes

$$\lambda + yA^a,\quad \mu + y'B^b,\quad \nu + y''C^c,\quad \text{etc.}$$

Cherchez donc les valeurs de y et y' pour que les deux racines

$$\lambda + yA^a \quad \text{et} \quad \mu + y'B^b$$

soient la même, et vous aurez, par l'équation du premier degré

$$\lambda + yA^a = \mu + y'B^b,$$

une racine μ' qui satisfera à

$$x^D - 1 = \mathfrak{M}(A^a.B^b),$$

et par conséquent sera de la forme

$$\mu' + z.A^a.B^b.$$

Déterminez maintenant z et y'' pour que les deux racines

$$\mu' + z.A^a.B^b \quad \text{et} \quad \nu + y''.C^c$$

soient la même, ce qui se fera par l'équation du premier degré

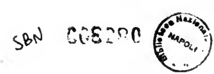
$$\mu' + z.A^aB^b = \nu + y''.C^c,$$

et vous aurez une nouvelle racine qui satisfera à l'équation

$$x^D - 1 = \mathfrak{M}(A^a.B^b.C^c);$$

et ainsi de suite.

IMPRIMERIE DE BACHELIER,
rue du Jardinet, 12.



72


BIBLIOTECA